

【特許請求の範囲】

【請求項1】

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理装置であり、

情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段と、

前記暗号処理手段において復号されたコンテンツの再生制御処理を実行する再生制御手段を有し、

前記暗号処理手段は、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力し、

10

前記再生制御手段は、前記暗号処理手段から受領する前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出するとともに、復号コンテンツ内に格納された第2のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする情報処理装置。

【請求項2】

前記再生制御手段は、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、第1の編集スタジオコードと第1の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードを取得し、編集スタジオコードおよび情報記録媒体製造者コード各々について、第1コードと第2コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする請求項1に記載の情報処理装置。

20

【請求項3】

前記復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル(PMT: Program Map Table)に含まれる編集スタジオコード(ASC: Authoring Studio Code)と情報記録媒体製造者コード(DMC: Disc Manufacturer Code)であることを特徴とする請求項2に記載の情報処理装置。

30

【請求項4】

前記再生制御手段は、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得し、

編集スタジオコード(ASC)および情報記録媒体製造者コード(DMC)各々について、第1コードと第2コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする請求項1に記載の情報処理装置。

40

【請求項5】

前記暗号処理手段は、

前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキーKb2を生成し、生成した第2ブロックキーKb2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成を有することを特徴とする請求項1

50

に記載の情報処理装置。

【請求項6】

前記暗号処理手段は、

前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのEKB(Enabling Key Block)の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行する構成を有することを特徴とする請求項1に記載の情報処理装置。

【請求項7】

前記暗号処理手段は、

前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御手段に出力し、

前記再生制御手段は、

前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項8】

前記暗号処理手段は、

前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体IDを読み取り、該情報記録媒体IDの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項9】

前記暗号処理手段は、

前記情報記録媒体IDに付加された電子署名の検証処理を実行し、該情報記録媒体IDの改竄のないことの確認を条件として、前記情報記録媒体IDの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項8に記載の情報処理装置。

【請求項10】

暗号化コンテンツを格納した情報記録媒体であり、

コンテンツの利用ライセンスを持つユーザデバイスに格納されたデバイスキーによってのみ復号処理可能な暗号化キーブロックとしてのEKB(Enabling Key Block)と、

前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードの暗号化情報としての暗号化エンティティコードと、

前記製造ルートのエンティティに対応して設定された第2のコード情報を含む暗号化コンテンツと、

を格納した構成を有することを特徴とする情報記録媒体。

【請求項11】

前記暗号化エンティティコードは、前記EKBの復号によって取得可能な鍵を適用した処理によって算出可能なコードであることを特徴とする請求項10に記載の情報記録媒体。

【請求項12】

前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードは、編集スタジオコード(ASC:Authoring Studio Code)と情報記録媒体製造者コード(DMC:Disc Manufacturer Code)を含み、

前記暗号化コンテンツにも、編集スタジオコード(ASC:Authoring Studio Code)と情報記録媒体製造者コード(DMC:Disc Manufacturer Code)を含む構成であることを特徴とする請求項10に記載の情報記録媒

10

20

30

40

50

体。

【請求項13】

前記暗号化コンテンツに含まれる前記第2のコード情報は、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を含むプログラムマップテーブル（PMT：Program Map Table）であることを特徴とする請求項10に記載の情報記録媒体。

【請求項14】

前記暗号化コンテンツに含まれる前記第2のコード情報は、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を含む電子透かし情報であることを特徴とする請求項10に記載の情報記録媒体。

10

【請求項15】

前記情報記録媒体は、
暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードと、

前記第1シードに基づいて生成される第1ブロックキーKb1に基づいて暗号化された鍵生成情報としての暗号化第2シードと、

前記第2シードに基づいて生成される第2ブロックキーKb2に基づいて暗号化された暗号化コンテンツと、

を格納した構成であることを特徴とする請求項10に記載の情報記録媒体。

【請求項16】

20

前記情報記録媒体は、さらに、

前記情報記録媒体の製造ルートのエンティティである編集スタジオ（AS：Authoring Studio）と情報記録媒体製造者（DM：Disc Manufacturer）各々が生成した鍵生成情報を含み、

前記情報記録媒体製造者の鍵生成情報と前記第1シードとに基づいて前記第1ブロックキーKb1が生成され、

前記編集スタジオの鍵生成情報と前記第2シードとに基づいて前記第2ブロックキーKb2が生成される構成であることを特徴とする請求項15に記載の情報記録媒体。

【請求項17】

コンテンツを格納した情報記録媒体の製造および利用管理を実行するコンテンツ管理システムであり、

30

コンテンツ管理エンティティとしての管理センタが、コンテンツ編集を実行するコンテンツ編集エンティティと、コンテンツを格納した情報記録媒体の製造を実行する情報記録媒体製造エンティティとに対応するコード情報として編集スタジオコード（ASC：Authoring Studio Code）と情報記録媒体製造者コード（DMC：Disc Manufacturer Code）を生成し、

前記コンテンツ編集エンティティは、前記編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を前記管理センタから受領して暗号化コンテンツ中に埋め込み、

前記情報記録媒体製造エンティティは、前記編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を暗号化した暗号化コードを前記管理センタから受領して該暗号化コードを情報記録媒体に格納する処理を実行する構成を有することを特徴とするコンテンツ管理システム。

40

【請求項18】

前記コンテンツ編集エンティティは、

鍵生成情報としての記録シード（REC SEED）を生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第2シード）とに基づいて第2ブロックキーKb2を生成し、該第2ブロックキーKb2に基づくコンテンツ暗号化を実行し、

前記情報記録媒体製造エンティティは、

鍵生成情報としての物理インデックスを生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第1シード）に基づいてブロックキーKb1を生成し、該第1ブロック

50

キー K b 1 に基づく前記第 2 シードの暗号化を実行する構成であることを特徴とする請求項 17 に記載のコンテンツ管理システム。

【請求項 19】

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理方法であり、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、

前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第 1 のエンティティコードを算出するとともに、復号コンテンツ内に格納された第 2 のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、

を有することを特徴とする情報処理方法。

【請求項 20】

前記再生制御ステップは、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、第 1 の編集スタジオコードと第 1 の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第 2 の編集スタジオコードと第 2 の情報記録媒体製造者コードを取得するステップと、

編集スタジオコードおよび情報記録媒体製造者コード各々について、第 1 コードと第 2 コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、

を含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 21】

前記復号コンテンツ内に格納された第 2 の編集スタジオコードと第 2 の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル (PMT: Program Map Table) に含まれる編集スタジオコード (ASC: Authoring Studio Code) と情報記録媒体製造者コード (DMC: Disc Manufacturer Code) であることを特徴とする請求項 20 に記載の情報処理方法。

【請求項 22】

前記再生制御ステップは、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を取得するステップと、

編集スタジオコード (ASC) および情報記録媒体製造者コード (DMC) 各々について、第 1 コードと第 2 コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、

を含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 23】

前記暗号処理ステップは、

前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第 1 シードに基づいて第 1 ブロックキー K b 1 を生成し、生成した第 1 ブロックキー K b 1 に基づいて情報記録媒体に格納された暗号化第 2 シードの復号処理を実行して第 2 シードを取得し、取得した第 2 シードに基づいて第 2 ブロックキー K b 2 を生成し、生成した第 2 ブロックキー K b 2 に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップを含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 24】

前記暗号処理ステップは、
前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしての EKB (Enabling Key Block) の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行するステップを含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 25】

前記暗号処理ステップは、
前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、
前記再生制御ステップは、
前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエントリティに対応して設定された暗号化エントリティコードの復号処理を実行して第 1 のエントリティコードを算出するステップを含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 26】

前記暗号処理ステップは、
前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体 ID を読み取り、該情報記録媒体 ID の要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする請求項 19 に記載の情報処理方法。

【請求項 27】

前記暗号処理ステップは、
前記情報記録媒体 ID に付加された電子署名の検証処理を実行し、該情報記録媒体 ID の改竄のないことの確認を条件として、前記情報記録媒体 ID の要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする請求項 26 に記載の情報処理方法。

【請求項 28】

情報記録媒体に格納された暗号化データの復号および再生制御を実行するコンピュータ・プログラムであり、
前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、
前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエントリティに対応して設定された暗号化エントリティコードの復号処理を実行して第 1 のエントリティコードを算出するとともに、復号コンテンツ内に格納された第 2 のエントリティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、
を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムに関する。詳細には、情報記録媒体を利用したデータ記録再生処理における不正なコンテンツ利用を防止する情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはCD（Compact Disc）、DVD（Digital Versatile Disc）、MD（Mini Disc）等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、CDプレーヤ、DVDプレーヤ、MDプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

【0003】

10

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

【0004】

特に、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをCD-R等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

20

【0005】

特に、近年開発されたDVD等の大容量型記録媒体は、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。

【0006】

デジタル記録再生を行う記録装置やデジタル記録媒体によれば、画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通すると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

30

【0007】

例えば、DVDプレーヤでは、CSS（Content Scramble System）が採用されている。CSSでは、DVD-ROM（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

40

【0008】

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するための鍵を有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、CSSの構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

【0009】

しかしながら、DVD-ROMで採用されているCSSは、ユーザによるデータの書き込

50

みが不可能な記録媒体を対象としており、ユーザによるデータの書き込みが可能な記録媒体への適用については考慮されていない。

【0010】

即ち、データの書き込みが可能な記録媒体に記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0011】

さらに、CSSの暗号を破るソフトウェアプログラム、例えばDeCSSソフトウェアがインターネット上で配布されており、このプログラムを適用することで、DVD Videoの暗号を解いて平文の状態で記録型DVDへ書き込むことが可能になっている。DeCSSが出現した背景は、本来解読防止のための実装時の隠蔽対応が義務付けられているはずのCSS復号用の鍵データを何の対処もしないまま設計されたDVDプレーヤー・ソフトウェアがリバースエンジニアされて鍵データが解読されたことであり、解読された鍵データから連鎖的にCSSアルゴリズム全体が解読されたという経緯である。

10

【0012】

鍵データを含む著作権保護技術実行プログラムをPC上で実行されるアプリケーションプログラムへ実装する際には、著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的であるが、対タンパー性の強度を示す指標は無く、そのためどれほどリバースエンジニアリングへの対応を行うかは個々のインプレメンターの判断や実力に委ねられているのが実情であり、CSSの場合には結果として破られてしまい、不正なコピーコンテンツの氾濫を招く結果となっている。

20

【0013】

CSS以外にも、DVD規格で採用されている著作権保護技術（コピーコントロール技術）として、CPPM（Content Protection for Pre-recorded Media）とCPRM（Content Protection for Recordable Media）がある。CPPMは、再生専用のメディア（Pre-recorded Media）用に開発されたコピーコントロール技術であり、CPRMは、記録可能なメディア（Recordable Media）用に開発されたコピーコントロール技術である。これらは、メディア（例えばディスク）側にメディアキーブロックと呼ばれる鍵情報を格納し、一方、再生装置、PC等、デバイス側にデバイスキーを格納し、これらの鍵の組み合わせにより、コピーコントロールを行うものである。

30

【0014】

しかし、このようなCPRMや、CPPMにおいても、デバイスとしてのPCやメディアとしてのディスク内に格納された鍵情報の漏洩の危険性を解消するといった根本的な問題解決を図る技術についての提案はなく、CPRMや、CPPMにおいても、鍵の漏洩によってコピーコントロールシステムが崩壊する危険性を常に有しているのが現状である。

【0015】

なお、コンテンツの不正利用を防止する技術として、本出願人は、例えば特許文献1および特許文献2において、記録媒体に格納するコンテンツのデータブロック毎に異なる鍵を適用した暗号処理技術を提案した。すなわち、データブロック毎の鍵生成情報としてシードを設定し、ブロック毎に設定したシードを暗号鍵の生成に適用する構成により、従来の1つの鍵のみによるコンテンツ暗号化を複雑化して、暗号アルゴリズムの解読困難性を高めたものである。

40

【0016】

しかし、上述の構成において、データブロック毎の鍵生成情報としてシードは、記録媒体に格納された情報そのものを使用したものであり、前述のCSSと同様の経緯で鍵データが解読され、解読された鍵データとデータブロック毎に異なるシードからブロックキーが導かれることによりコンテンツの漏洩を引き起こす懸念が皆無とはいえない。

【0017】

また、コンテンツを格納したCD、DVD等の情報記録媒体を製造する場合、コンテンツ

50

編集者と、ディスク製造者とはそれぞれ別のエンティティとして存在するのが通常であり、コンテンツ編集者において、あるいはディスク製造者の一方において適切な管理を実行しても不十分であり、双方のエンティティにおいて適切な管理を行うことが必要となる。

【0018】

しかし、現状においては、コンテンツを格納した情報記録媒体の製造ルートにおけるコンテンツ管理、鍵情報管理を総括的にかつ効率的に実行する適切な構成が実現されているとは言い難く、不正なコピー媒体が市場に流通した場合、その情報漏洩ルートを追跡することは困難となるというのが現状であった。特にコンテンツ編集者自身によるコンテンツの盗難行為やディスク製造者自身による盗難されたコンテンツの製造の結果として市場に流通する媒体は正規品との判別が困難であり、不正な媒体の市場への流通は一層深刻な状況となりつつある。

10

【0019】

【特許文献1】

特許公開2001-351324号公報

【特許文献2】

特許公開2002-236622号公報

【0020】

【発明が解決しようとする課題】

本発明は、上述の従来技術における問題点を鑑みてなされたものであり、DVD、CD等の各種情報記録媒体に格納したコンテンツを再生装置、PC（パーソナルコンピュータ）等の情報処理装置において利用する構成において、記録媒体に格納するコンテンツの暗号化に適用する鍵情報の漏洩を困難とし、鍵解読、暗号アルゴリズムの解読の困難性を高めることを実現するとともに、不正に複製されたDVD、CD等の各種情報記録媒体が流通した場合において、その流通経路の効率的な追跡を可能とし、不正品の再生制限を可能とした情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

20

【0021】

【課題を解決するための手段】

本発明の第1の側面は、

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理装置であり、

30

情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段と、

前記暗号処理手段において復号されたコンテンツの再生制御処理を実行する再生制御手段を有し、

前記暗号処理手段は、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力し、

前記再生制御手段は、前記暗号処理手段から受領する前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出するとともに、復号コンテンツ内に格納された第2のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする情報処理装置にある。

40

【0022】

さらに、本発明の情報処理装置の一実施態様において、前記再生制御手段は、前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、第1の編集スタジオコードと第1の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードを取得し、編集スタジオコードおよび情報記録媒体製造者コード各々について、第1コードと第2コード間の照

50

合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする。

【0023】

さらに、本発明の情報処理装置の一実施態様において、前記復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル(PMT: Program Map Table)に含まれる編集スタジオコード(ASC: Authoring Studio Code)と情報記録媒体製造者コード(DMC: Disc Manufacturer Code)であることを特徴とする。

【0024】

さらに、本発明の情報処理装置の一実施態様において、前記再生制御手段は、前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得し、編集スタジオコード(ASC)および情報記録媒体製造者コード(DMC)各々について、第1コードと第2コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする。

10

【0025】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキーKb2を生成し、生成した第2ブロックキーKb2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成を有することを特徴とする。

20

【0026】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのEKB(Enabling Key Block)の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行する構成を有することを特徴とする。

30

【0027】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御手段に出力し、前記再生制御手段は、前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出する構成であることを特徴とする。

40

【0028】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体IDを読み取り、該情報記録媒体IDの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【0029】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体IDに付加された電子署名の検証処理を実行し、該情報記録媒体IDの改竄のないことの確認を条件として、前記情報記録媒体IDの要素としてのディスク固有シードを取

50

得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【0030】

さらに、本発明の第2の側面は、

暗号化コンテンツを格納した情報記録媒体であり、

コンテンツの利用ライセンスを持つユーザデバイスに格納されたデバイスキーによってのみ復号処理可能な暗号化キープロックとしてのEKB (Enabling Key Block) と、

前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードの暗号化情報としての暗号化エンティティコードと、

前記製造ルートのエンティティに対応して設定された第2のコード情報を含む暗号化コンテンツと、

を格納した構成を有することを特徴とする情報記録媒体にある。

【0031】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化エンティティコードは、前記EKBの復号によって取得可能な鍵を適用した処理によって算出可能なコードであることを特徴とする。

【0032】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードは、編集スタジオコード(ASC: Authoring Studio Code)と情報記録媒体製造者コード(DMC: Disc Manufacturer Code)を含み、前記暗号化コンテンツにも、編集スタジオコード(ASC: Authoring Studio Code)と情報記録媒体製造者コード(DMC: Disc Manufacturer Code)を含む構成であることを特徴とする。

【0033】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化コンテンツに含まれる前記第2のコード情報は、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を含むプログラムマップテーブル(PMT: Program Map Table)であることを特徴とする。

【0034】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化コンテンツに含まれる前記第2のコード情報は、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を含む電子透かし情報であることを特徴とする。

【0035】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードと、前記第1シードに基づいて生成される第1ブロックキーKb1に基づいて暗号化された鍵生成情報としての暗号化第2シードと、前記第2シードに基づいて生成される第2ブロックキーKb2に基づいて暗号化された暗号化コンテンツと、を格納した構成であることを特徴とする。

【0036】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、前記情報記録媒体の製造ルートのエンティティである編集スタジオ(AS: Authoring Studio)と情報記録媒体製造者(DM: Disc Manufacturer)各々が生成した鍵生成情報を含み、前記情報記録媒体製造者の鍵生成情報と前記第1シードとに基づいて前記第1ブロックキーKb1が生成され、前記編集スタジオの鍵生成情報と前記第2シードとに基づいて前記第2ブロックキーKb2が生成される構成であることを特徴とする。

【0037】

さらに、本発明の第3の側面は、

コンテンツを格納した情報記録媒体の製造および利用管理を実行するコンテンツ管理システムであり、

コンテンツ管理エンティティとしての管理センタが、コンテンツ編集を実行するコンテンツ編集エンティティと、コンテンツを格納した情報記録媒体の製造を実行する情報記録媒体製造エンティティとに対応するコード情報として編集スタジオコード（ASC: Authoring Studio Code）と情報記録媒体製造者コード（DMC: Disc Manufacturer Code）を生成し、

前記コンテンツ編集エンティティは、前記編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を前記管理センタから受領して暗号化コンテンツ中に埋め込み、前記情報記録媒体製造エンティティは、前記編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を暗号化した暗号化コードを前記管理センタから受領して該暗号化コードを情報記録媒体に格納する処理を実行する構成を有することを特徴とするコンテンツ管理システムにある。

10

【0038】

さらに、本発明のコンテンツ管理システムの一実施態様において、前記コンテンツ編集エンティティは、鍵生成情報としての記録シード（RECORD SEED）を生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第2シード）とに基づいて第2ブロックキーKb2を生成し、該第2ブロックキーKb2に基づくコンテンツ暗号化を実行し、前記情報記録媒体製造エンティティは、鍵生成情報としての物理インデックスを生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第1シード）に基づいてブロックキーKb1を生成し、該第1ブロックキーKb1に基づく前記第2シードの暗号化を実行する構成であることを特徴とする。

20

【0039】

さらに、本発明の第4の側面は、

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理方法であり、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、

30

前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出するとともに、復号コンテンツ内に格納された第2のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、

を有することを特徴とする情報処理方法にある。

【0040】

さらに、本発明の情報処理方法の一実施態様において、前記再生制御ステップは、前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、第1の編集スタジオコードと第1の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードを取得するステップと、編集スタジオコードおよび情報記録媒体製造者コード各々について、第1コードと第2コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、を含むことを特徴とする。

40

【0041】

さらに、本発明の情報処理方法の一実施態様において、前記復号コンテンツ内に格納された第2の編集スタジオコードと第2の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル（PMT: Program Map Table）に含まれる編集スタジオコード（ASC: Authoring Studio Code）と情報記録媒体製造者コード（DMC: Disc Manufacturer Code）とを有することを特徴とする。

50

e)であることを特徴とする。

【0042】

さらに、本発明の情報処理方法の一実施態様において、前記再生制御ステップは、前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を取得するステップと、編集スタジオコード(ASC)および情報記録媒体製造者コード(DMC)各々について、第1コードと第2コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、を含むことを特徴とする。

10

【0043】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキーKb2を生成し、生成した第2ブロックキーKb2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップを含むことを特徴とする。

【0044】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのEKB(Enabling Key Block)の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行するステップを含むことを特徴とする。

20

【0045】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御ステップは、前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出するステップを含むことを特徴とする。

30

【0046】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体IDを読み取り、該情報記録媒体IDの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする。

【0047】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体IDに付加された電子署名の検証処理を実行し、該情報記録媒体IDの改竄のないことの確認を条件として、前記情報記録媒体IDの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする。

40

【0048】

さらに、本発明の第5の側面は、
情報記録媒体に格納された暗号化データの復号および再生制御を実行するコンピュータ・プログラムであり、
前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵

50

情報を生成して、前記再生制御手段に出力する暗号処理ステップと、
前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第1のエンティティコードを算出するとともに、復号コンテンツ内に格納された第2のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【0049】

【作用】

本発明においては、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【0050】

さらに、本発明の構成によれば、情報記録媒体に格納されたコンテンツは、シード情報（シード1）およびシード情報（シード2）によって生成されるブロック鍵Kb1、Kb2で暗号化され、シード情報（シード2）は、シード情報（シード1）を用いて生成される鍵、すなわちブロックキーKb1によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード2）の解析、シード情報（シード2）を適用して生成するブロックキーKb2の解析、ブロックキーKb2によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【0051】

さらに、本発明の構成によれば、コンテンツ編集エンティティが、鍵生成情報としての記録シード（RECS EED）を生成し、管理センタから受領する鍵情報、および鍵生成情報（第2シード）とに基づいて第2ブロックキーKb2を生成し、第2ブロックキーKb2に基づくコンテンツ暗号化を実行し、情報記録媒体製造エンティティが、鍵生成情報としての物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報（第1シード）に基づいてブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づく第2シードの暗号化を実行する構成とし、さらに、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製された場合には、コード検出による情報漏洩ルートの解析が可能となる。

【0052】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやDVD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0053】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0054】

【発明の実施の形態】

以下、本発明の情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムの詳細について説明する。

【0055】

〔記録媒体上のデータ記録構成および製造プロセス概要〕

まず、本発明に係る情報記録媒体に格納されるデータ構成および製造プロセス概要について説明する。情報記録媒体に格納された暗号化データは、データ記録再生装置や、PC（パーソナルコンピュータ）において読み取られ、復号、再生される。

【0056】

本発明の情報記録媒体に格納されるデータについて、図1を参照して説明する。図1には、ディスク状の情報記録媒体100を例として示す。なお、本発明における情報記録媒体は、光、磁気、半導体、フラッシュメモリ等、様々な形体の情報記録媒体を含み、ディスク状のものに限定されるものではない。 10

【0057】

図1に示すように、情報記録媒体100には、ディスクID101、物理インデックス102、暗号化コンテンツ103、記録シード（REC SEED）104、暗号鍵情報120が格納される。暗号鍵情報120は、情報記録媒体100のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域110に格納される。

【0058】

暗号鍵情報120には、情報記録媒体100に格納された暗号化コンテンツ103の復号、再生に必要な様々な鍵情報が含まれる。図1、図2を参照して、情報記録媒体に格納される情報の概要と、情報記録媒体の製造ルートについて説明する。 20

【0059】

図2に示すように、情報記録媒体に格納するコンテンツは、コンテンツ編集エンティティ（AS：Authoring Studio）330において編集され、その後、情報記録媒体製造エンティティ（DM：Disc Manufacturer）350において、ユーザに提供される媒体としてのCD、DVD等が大量に複製（レプリカ）されて、情報記録媒体100が製造され、ユーザに提供される。情報記録媒体100はユーザの情報処理装置200において再生される。

【0060】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ（TC：Trusted Center）300である。管理センタ（TC：Trusted Center）300は、コンテンツ編集エンティティ（AS：Authoring Studio）330、および情報記録媒体製造エンティティ（DM：Disc Manufacturer）350に対して様々な管理情報を提供し、コンテンツ編集エンティティ（AS：Authoring Studio）330、および情報記録媒体製造エンティティ（DM：Disc Manufacturer）350は、管理センタ（TC：Trusted Center）300から受領した管理情報に基づいて、コンテンツの編集、暗号化、鍵情報の、生成、格納処理などを行う。また、管理センタ（TC：Trusted Center）300は、ユーザの情報処理装置に格納するデバイスキーの管理、提供も行う。これらの各情報の詳細については後述する。 30 40

【0061】

図1に示す暗号鍵情報120には、情報記録媒体100に格納された暗号化コンテンツ103の復号、再生に必要な様々な鍵情報が含まれる。暗号鍵情報120は、管理センタ300が生成し、情報記録媒体製造エンティティ（DM：Disc Manufacturer）350に提供される。情報記録媒体製造エンティティ（DM：Disc Manufacturer）350は、管理センタ300から提供される暗号鍵情報120を情報記録媒体100のリードイン領域110に格納する。

【0062】

暗号鍵情報120には、コンテンツ再生に必要なとなるメディアキーKmを暗号化して格納 50

した暗号鍵ブロックとしてのEKB121、コンテンツまたはメディアに対応して設定される第1タイトルキー(Kt1)をメディアキーKmで暗号化した暗号化第1タイトルキーeKm(Kt1)122、第2タイトルキー(Kt2)をメディアキーで暗号化した暗号化第2タイトルキーeKm(Kt2)123、コンテンツ編集エンティティコード(ASC: Authoring Studio Code)を第2タイトルキーKt2で暗号化した暗号化ASC:eKt2(ASC)124、情報記録媒体製造者コード(DMC: Disc Manufacturer Code)を第2タイトルキー(Kt2)で暗号化した暗号化DMC:eKt2(DMC)125を含んでいる。

【0063】

EKB121は、有効化キーブロック(Enabling Key Block)であり、有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキーに基づく処理(復号)によってのみ、コンテンツの復号に必要なメディアキーを取得する鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式によって、ユーザデバイス(情報処理装置)のライセンスの有効性に基づく鍵取得を可能としたものであり、無効化(リボーク処理)されたユーザデバイスの鍵(メディアキー)取得を阻止可能としたものである。管理センタはEKBに格納する鍵情報の変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つEKBを生成することができる。

【0064】

階層型木構造を適用した暗号鍵等の暗号データ提供処理について、図を参照して説明する。図3の最下段に示すナンバ0~15が、例えばコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図3に示す階層ツリー(木)構造の各葉(リーフ: leaf)がそれぞれのデバイスに相当する。

【0065】

各デバイス0~15は、製造時あるいは出荷時、あるいはその後において、図1に示す階層ツリー(木)構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーからなるキーセット(デバイスキー(DNK: Device Node Key))をメモリに格納する。図3の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKR(ルートキー)から、最下段から2番目の節(ノード)に記載されたキー: KR~K111をノードキーとする。

【0066】

図3に示す木構造において、例えばデバイス0はリーフキーK0000と、ノードキー: K000、K00、K0、KRをデバイスキーとして所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0067】

また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0068】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対し

10

20

30

40

50

ては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはCD等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵を送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティティは、図3の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図3のツリー中に複数存在する。

【0069】

なお、ノードキー、リーフキーは、ある1つの管理センタ機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

【0070】

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はデバイスキー(DNK: Device Node Key)として共通のキーK00、K0、KRを含むデバイスキー(DNK: Device Node Key)を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00は、デバイス0, 1, 2, 3に共通する保有キーとなる。また、新たなキーKnewをノードキーK00で暗号化した値Enc(K00, Knew)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Knew)を解いて新たなキーKnewを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0071】

また、ある時点tにおいて、デバイス3の所有する鍵: K0011, K001, K00, K0, KRが例えば攻撃者(ハッカー)により解析されて露呈したことが発覚した場合、それ以降、システム(デバイス0, 1, 2, 3のグループ)で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation): tの更新キーであることを示す。

【0072】

更新キーの配布処理について説明する。キーの更新は、例えば、図4(A)に示す有効化キーブロック(EKB: Enabling Key Block)と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キーブロック(EKB)は、図4に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック(EKB)は、キー更新ブロック(KRB: Key Renewal Block)と呼ばれることもある。

【0073】

図4(A)に示す有効化キーブロック(EKB)には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布す

10

20

30

40

50

ることを目的として形成されたブロックデータである。図3から明らかなように、デバイス0、デバイス1は、更新ノードキーとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

【0074】

図4(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図4(A)の下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図4(A)の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4(A)の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。

10

【0075】

一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図4(A)の上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図4(A)の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4(A)の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0、1、2は更新した鍵 $K(t)R$ を得ることができる。なお、図4(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

20

【0076】

図3に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図4(B)の有効化キーブロック(EKB)を用いることで、更新ノードキー $K(t)00$ をデバイス0、1、2に配布することができる。

30

【0077】

図4(B)に示すEKBは、例えば特定のグループにおいてのみ取得可能なメディアキー K_m を配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0、1、2、3にのみ利用可能なメディアキー K_m を配布するとする。このとき、デバイス0、1、2、3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たなメディアキー K_m を暗号化したデータ $Enc(K(t)00, K(t)m)$ を図4(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0078】

すなわち、デバイス0、1、2はEKBを処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキー $K(t)m$ を得ることが可能になる。

40

【0079】

図5に、 t 時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキー $K(t)m$ をEKBの処理によって取得する処理例を示す。EKBには、 $K(t)00$ を用いてメディアキー $K(t)m$ を暗号化したデータ $Enc(K(t)00, K(t)m)$ と図4(B)に示すデータとが格納されているとする。ここでは、デバイス0の処理例を示す。

【0080】

図5に示すように、デバイス0は、記録媒体に格納されている世代： t 時点のEKBと自

50

分があらかじめ格納しているノードキー $K000$ を用いて上述したと同様の EKB 処理により、ノードキー $K(t)00$ を生成する。さらに、復号した更新ノードキー $K(t)00$ を用いて暗号化データ $Enc(K(t)00, K(t)m)$ を復号して更新メディアキー $K(t)m$ を取得する。

【0081】

また、別の例としてツリー構造のノードキーの更新は不必要で、時点 t でのメディアキー $K(t)m$ のみを必要な機器が得られればよいという場合もある。この場合、下記のような方式とすることができる。

【0082】

いま、図3の例と同様にデバイス0, 1, 2にのみメディアキー $K(t)m$ を送りたいとする。このとき EKB は、

バージョン (Version) : t

インデックス 暗号化キー

000 $Enc(K000, K(t)m)$

0010 $Enc(K0010, K(t)m)$

となる。

【0083】

デバイス0, 1は $K000$ を用いて、またデバイス2は $K0010$ を用いて上記 EKB のうちの1つの暗号文を復号することによりコンテンツ鍵を得ることができる。このようにすることにより、ノードキーの更新は行えないものの必要な機器にコンテンツ鍵を与える方法をより効率よく（すなわち、 EKB に含まれる暗号文数を減らして EKB のサイズを小さくするとともに管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

【0084】

図1に戻り、情報記録媒体100に格納されるその他のデータの詳細について説明する。ディスクID101は、情報記録媒体固有の識別子としての情報記録媒体IDである。管理センタ300が生成して情報記録媒体製造エンティティ350に渡す管理情報であり、ディスク1枚毎に異なるIDである。例えば、管理センタ300はディスク1枚毎に異なるシード (S) を生成し、改竄検証用の電子署名 (Sig) を付加したデータ (S, Sig) を管理センタが許容したディスク枚数分生成して情報記録媒体製造エンティティ350に提供する。情報記録媒体製造エンティティ350は、ディスク毎に異なるID情報 (S, Sig) を情報記録媒体 (ディスク) に格納する。

【0085】

コンテンツ再生を実行するユーザの情報処理装置においては、情報記録媒体 (ディスク) に格納されたID情報 (S, Sig) を読み取り、署名検証処理によりIDの改竄のないことの確認を条件として、コンテンツ復号プロセスに移行する。なお、署名は公開鍵暗号方式に基づく署名、またはMAC等の共通鍵暗号方式による署名等の利用が可能である。公開鍵暗号方式に基づく署名を適用する場合は、管理センタ300は、秘密鍵による署名生成を実行し、各ユーザの情報処理装置では、管理センタ300の公開鍵による署名検証を実行する。共通鍵方式の場合は、管理センタ、ユーザデバイス双方において共通の署名用鍵を保有し、署名生成、検証処理を実行する。ユーザの情報処理装置 (ユーザデバイス) における処理については後述する。

【0086】

図1に示す情報記録媒体に格納される物理インデックス102は、情報記録媒体製造エンティティ350が生成して、情報記録媒体に格納する。記録シード (REC SEED) 104は、コンテンツ編集エンティティ330が生成して、情報記録媒体製造エンティティ350に渡されて情報記録媒体に格納する値である。

【0087】

暗号化コンテンツ103は、暗号化コンテンツ中に、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) とを含むプログラムマップテーブルPMT (Prog

ram Map Table) が格納される。PMTは編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)を含む情報であり、コンテンツ編集エンティティ330においてコンテンツに対して埋め込まれる。さらに、暗号化コンテンツ103には、電子透かし(WM: Water Mark)としても、コンテンツ編集エンティティコード(ASC: Authoring Studio Code)、情報記録媒体製造者コード(DMC: Disc Manufacturer Code)が格納される。これらのコード埋め込みは、管理センタ300において行われる。情報記録媒体に対する様々なデータ埋め込み処理の詳細なシーケンスについては、後述する。

【0088】

情報記録媒体に格納される暗号化コンテンツは、例えばMPEG-2システムで規定されている符号化データとしてのトランスポートストリーム(TS)として構成される。トランスポートストリームは、1本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのATS(Arrival Time Stamp: 着信時刻スタンプ)が設定されている。このタイムスタンプは、MPEG-2システムで規定されている仮想的なデコーダであるTSTD(Transport Stream System Target Decoder)を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたATSによって出現タイミングを制御して、復号、再生を行う。

【0089】

例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【0090】

図6を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号再生処理の概要を説明する。情報記録媒体に格納されるデータは暗号化データであり、再生を行う場合には、復号処理を行うことが必要となる。図6(a)が情報記録媒体に格納されるデータ記録構成である。18バイトの制御データ(User Control Data)と、2048バイトのユーザデータ(User Data)が1つのセクタデータとして構成され、例えば3セクタ分のデータが1つの暗号処理単位として規定される。なおここで説明するバイト数や、処理単位は1つの代表例であり、制御データ、ユーザデータのバイト数や、処理単位の設定は、様々な設定が可能である。

【0091】

(b)は、暗号処理単位である1ユニット(1AU: Aligned Unit)の構成を示す。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である1AU(Aligned Unit)を抽出する。

【0092】

暗号処理単位である1ユニット(1AU)には、(c)暗号化構成に示すように、ブロックキーKb1によって暗号化された領域、ブロックキーKb2によって暗号化された領域が含まれる。ブロックキーKb1とKb2によって二重に暗号化された領域を含める構成としてもよい。ブロックキーを生成するためには、鍵生成情報としてのシード情報が必要となる。シード情報(シード1)はブロックキーKb1を生成するための鍵生成情報であり、シード情報(シード2)はブロックキーKb2を生成するための鍵生成情報である。これらは、制御データ領域、あるいはユーザデータ領域に格納される。図6(c)に示すシード情報の格納態様、暗号化態様は一例であり、後段において、複数の構成例について説明する。

【0093】

ユーザデータ領域に格納された暗号化コンテンツを復号するためには、情報記録媒体に格納されたシード情報を読み取って、シード情報に基づく鍵を生成することが必要となる。

【0094】

図6(c)に示すように、ブロックキーKb1を生成するために必要となるシード情報(シード1)と、ブロックキーKb2を生成するために必要となるシード情報(シード2)とを情報記録媒体上に格納するとともに、一方のシード情報(シード2)をシード情報(シード1)によって生成されるブロックキーKb1によって暗号化して格納している。また、暗号化コンテンツ中に、電子透かし(WM:Water Mark)として、コンテンツ編集エンティティコード(ASC:Authoring Studio Code)、情報記録媒体製造者コード(DMC:Disc Manufacturer Code)が格納される。

【0095】

このように、2つの異なる鍵を適用した暗号化処理を実行したデータを記録媒体に格納し、再生処理において2つの異なる鍵を適用した復号処理を行う。すなわち、所定の暗号処理単位毎に異なる鍵生成情報であるシード1、シード2を適用した暗号処理によりブロックキーKb1、Kb2を生成して復号処理を実行する。

【0096】

1処理単位毎の復号処理の後、復号されたトランスポートストリームパッケージがMP EG-2デコーダに入力されデコード処理が実行されてコンテンツ再生が行なわれる。1つの処理単位(3セクタ)には、例えば32個のトランスポートストリーム(TS)パッケージが含まれる。すなわち、 $32 \times 192 = 6144$ バイトデータが1つの暗号化および復号処理単位とされる。なお、処理単位の設定は、様々な設定が可能である。

【0097】

復号再生時には、各処理単位毎に2つのシード情報(シード1、シード2)を情報記録媒体から取得し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し、生成したブロックキーKb1、Kb2を用いて復号処理がなされて、コンテンツ再生が行われる。

【0098】

また、コンテンツの記録時には、復号再生処理と逆のプロセスが実行され、各処理単位毎に2つのシード情報(シード1、シード2)を設定し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し生成したブロックキーKb1、Kb2を用いて暗号化処理がなされて、コンテンツ記録が行われる。

【0099】

【0100】

[情報処理装置構成]

図7は、上述した暗号化コンテンツ態様を持つコンテンツの記録再生処理を実行する情報処理装置200の一実施例構成を示すブロック図である。情報処理装置200は、入出力I/F(Interface)220、MP EG(Moving Picture Experts Group)コーデック230、A/D、D/Aコンバータ241を備えた入出力I/F(Interface)240、暗号処理手段250、再生制御処理手段255、ROM(Read Only Memory)260、CPU(Central Processing Unit)270、メモリ280、記録媒体295のドライブ290、さらにトランスポートストリーム処理手段(TS処理手段)298を有し、これらはバス210によって相互に接続されている。

【0101】

入出力I/F220は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス210上に出力するとともに、バス210上のデジタル信号を受信し、外部に出力する。MP EGコーデック230は、バス210を介して供給されるMP EG符号化されたデータを、MP EGデコードし、入出力I/F240に出力するとともに、入出力I/F240から供給されるデジタル信号をMP EGエンコードしてバス210上に出力する。入出力I/F240は、A/D、D/Aコンバータ241を内蔵している。入出力I/F240は、外部から供給されるコンテンツとしてのア

10

20

30

40

50

ナログ信号を受信し、A/D、D/Aコンバータ241でA/D (Analog to Digital) 変換することで、デジタル信号として、MPEGコーデック230に出力するとともに、MPEGコーデック230からのデジタル信号を、A/D、D/Aコンバータ241でD/A (Digital to Analog) 変換することで、アナログ信号として、外部に出力する。

【0102】

暗号処理手段250は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス210を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス210上に出力する構成を持つ。再生制御処理手段255は、コンテンツ再生において検証すべき各種処理を実行して、再生条件を満足しない場合には、コンテンツ再生の停止を行う。暗号処理手段250および再生制御処理手段255の処理の詳細については後述する。

10

【0103】

なお、暗号処理手段250は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。図においては、暗号処理手段250、再生制御処理手段255をそれぞれ個別のブロックとして示してあるが、これらはたとえばCPU270の制御の下に実行するプログラムに基づいて実行する処理とすることも可能である。

【0104】

ROM260は、例えば、情報処理装置ごとに固有の、あるいは、複数の情報処理装置のグループごとに固有のデバイスキーや、相互認証時に必要とする認証キーを記憶している。デバイスキーは、例えば鍵配信ツリー構成に基づいて提供される暗号化鍵ブロック情報としてのEKB (Enabling Key Block) を復号してメディアキーを取得するために用いられる。すなわち、デバイスキーは、メディアキー生成情報として適用される。

20

【0105】

CPU270は、メモリ280に記憶されたプログラムを実行することで、MPEGコーデック230や暗号処理手段250等を制御する。メモリ280は、例えば、不揮発性メモリで、CPU270が実行するプログラムや、CPU270の動作上必要なデータを記憶する。メモリ280が不揮発性メモリの場合、デバイスキーを記憶することも可能であり、以降の実施例ではデバイスキーはメモリ280へ格納するとして説明をする。ドライブ290は、デジタルデータを記録再生可能な記録媒体295を駆動することにより、記録媒体295からデジタルデータを読み出し (再生し)、バス210上に出力するとともに、バス210を介して供給されるデジタルデータを、記録媒体295に供給して記録させる。

30

【0106】

記録媒体295は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはフラッシュROM、MRAM、RAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、図1を参照して説明した各種データを格納した情報記録媒体である。本実施の形態では、ドライブ290に対して着脱可能な構成であるとする。但し、記録媒体295は、情報処理装置200に内蔵する構成としてもよい。

40

【0107】

トランスポートストリーム処理手段 (TS処理手段) 298は、複数のコンテンツが多重化されたトランスポートストリームから特定のコンテンツに対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体295に格納するためのデータ処理を実行し、また、記録媒体295からの暗号化コンテンツの復号再生時には、トランスポートストリームの出現タイミング制御を行なう。

【0108】

トランスポートストリームには、前述したように、各トランスポートパケットの出現タイ

50

ミング情報としてのA T S (A r r i v a l T i m e S t a m p : 着信時刻スタンプ) が設定されており、M P E G 2 デコーダによる復号時にA T S によってタイミング制御を実行する。トランスポートストリーム処理手段(T S 処理手段) 2 9 8 は、例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【0109】

本発明の情報処理装置200は、例えば上述のトランスポートストリームによって構成される暗号化コンテンツの記録再生を実行する。これらの処理の詳細については、後段で説明する。なお、図7に示す暗号処理手段250、TS処理手段298は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する1つのワンチップLSIとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。さらには、ドライブ290、記録媒体295を除く全てのブロックをワンチップLSIとして構成してもよく、また、これらの機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよく、これにより情報処理装置200の改造によるセキュリティ機能の無効化に対するロバストネスを向上させることが出来る。

【0110】

[データ再生処理]

次に、記録媒体に格納された暗号化データの復号処理および再生制御処理について説明する。図8に示すように、情報処理装置200におけるコンテンツ再生は、暗号処理手段250における暗号化コンテンツの復号処理と、再生制御手段255における再生制御処理の2つのステップを含む。

【0111】

情報記録媒体100から各種の情報が読み取られ、暗号処理手段250における暗号化コンテンツの復号処理が実行され、復号コンテンツが再生制御手段255に渡され、再生条件判定処理が実行され、再生条件を満足する場合にのみコンテンツ再生が継続して実行され、再生条件を満足しない場合には、コンテンツ再生が停止される。

【0112】

まず、暗号処理手段250における暗号化コンテンツの復号処理の詳細について、図9以下を参照して説明する。

【0113】

コンテンツ復号プロセスでは、まず、暗号処理手段250は、メモリに格納しているデバイスキー410を読み出す。デバイスキー410は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。

【0114】

次に、暗号処理手段250は、ステップS11において、デバイスキー410を適用して情報記録媒体100に格納されたメディアキー格納EKBの復号処理を実行して、メディアキーKmを取得する。

【0115】

次に、ステップS12において、情報記録媒体100に格納されたメディアキーKmにより暗号化された暗号化第2タイトルキーeKm(Kt2)を、ステップS11におけるEKB処理で取得したメディアキーKmを用いて復号し、第2タイトルキーKt2を取得する。第2タイトルキーKt2は、再生制御処理手段255に出力される。

【0116】

ステップS13において、情報記録媒体100に格納されたメディアキーKmにより暗号化された暗号化第1タイトルキーeKm(Kt1)を、ステップS11におけるEKB処理で取得したメディアキーKmを用いて復号し、第1タイトルキーKt1を取得する。

【0117】

次にステップS14で、情報記録媒体100に格納されたディスクIDからディスク固有シード(S)を取得する。暗号処理手段250は、情報記録媒体100に格納された識別情報としてのディスクID(Disc ID)404を読み出して、ディスクID404の検証処理を実行する。ディスクIDは、管理センタ300が生成したディスク1枚毎に異なるシードSと改竄検証用の電子署名(Sig)を持つデータ(S, Sig)である。暗号処理手段250は、情報記録媒体100に格納されたID情報(S, Sig)を読み取り、署名検証処理によりIDの改竄のないことを確認する。公開鍵暗号方式に基づく署名の場合は、管理センタ300の公開鍵による署名検証を実行する。共通鍵方式の場合は、共通鍵により署名検証処理を実行する。署名検証処理によりIDの改竄のないことを確認を条件として、ステップS14で、情報記録媒体100に格納されたディスクIDからディスク固有シードSを取得する。署名検証処理によりIDの改竄があると判定した場合は、コンテンツ復号処理は停止する。

10

【0118】

署名検証処理によりIDの改竄のないことを確認がなされると、次に、ステップS15において、ディスク固有シードSと、タイトルキーK2を用いて、ディスク固有キー(Disc Unique Key)Kdを生成する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、例えば、図10(a)に示すように、ディスク固有シードSを入力値とし、共通鍵暗号方式であるAES(Advanced Encryption Standard)暗号を、タイトルキーK2を暗号鍵として実行する方法や、図10(b)に示すように、FIPS 180-1で定められているハッシュ関数SHA-1に、タイトルキーK2とディスク固有シードSとのビット連結により生成されるデータを入力し、その出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する方法などが適用できる。

20

【0119】

さらに、暗号処理手段250は、ステップS13において生成した第1タイトルキーKt1と、情報記録媒体100から読み出した物理インデックス406とに基づいて、ステップS16において、第1記録キー(RECキー)K1を生成し、また、ステップS15において生成したディスク固有キーKdと、情報記録媒体100から読み出した記録シード(REC SEED)405とに基づいて、ステップS17において、第2記録キー(RECキー)K2を生成する。これらの各キーの生成処理においてもAES暗号処理等、ハッシュ関数、縮約関数などが適宜使用される。

30

【0120】

記録キーK1、K2は、上述の再生処理プロセスにおいて使用することが必要となるが、コンテンツを情報記録媒体に記録する暗号処理においても適用される鍵、記録処理については後述する。

【0121】

ステップS16、S17において2つの記録キー(RECキー)1, 2を生成すると、次に、ステップS18から、情報記録媒体100に格納された暗号化コンテンツ407の読み出しおよび2つのブロックキーKb1, Kb2による復号処理が開始される。

【0122】

ステップS18において、情報記録媒体100に格納された暗号化コンテンツ407から制御情報(UCD: User Control Data)に含まれるシード情報(シード1)が取得され、ステップS19において、シード情報(シード1)と、ステップS16において生成した第1記録キーK1とに基づく暗号処理を実行してブロックキーKb1を生成する。

40

【0123】

ステップS19のブロックキーKb1の生成処理以降に実行する処理について、図9とともに図11を参照して説明する。

【0124】

図11において、復号処理は、処理単位420を単位として実行される。この処理単位は

50

、先に図6を参照して説明した(b)処理単位に相当する。すなわち、暗号処理単位である1ユニット(1AU: Aligned Unit)である。情報記録媒体100に格納された暗号化データの再生を実行する暗号処理手段250は、制御データ内のフラグに基づいて、暗号処理単位である1AU (Aligned Unit)を抽出する。

【0125】

処理単位420には、18バイトの制御データ(UCD: User Control Data)421と、6144バイトのユーザデータ(暗号化コンテンツを含む)が含まれる。6144バイトのユーザデータは、トランスポートストリームパケットの単位である192バイト毎に分割される。ユーザデータの先頭のTSパケット422と、後続の5952バイトのTSパケット群423を分離して説明する。この例では、シード情報(シード1)431が制御データ421に格納され、シード情報(シード2)432がユーザデータ内の先頭のTSパケット422内に暗号化されて格納された例である。

10

【0126】

なお、シード情報としての、シード1、シード2の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

【0127】

図11において、図9の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【0128】

ステップS19(図9、図11)においては、情報記録媒体の制御データ内から読み出したシード情報(シード1)431をAES暗号処理部に入力し、先のステップS16において生成した記録キーK1を適用したAES暗号処理を実行しブロックキーKb1を生成する処理を実行する。なお、図11においてAES_Gは、AES暗号処理を適用した鍵生成(Key Generation)処理を示し、AES_Dは、AES暗号処理を適用したデータ復号(Decryption)処理を示している。

20

【0129】

ステップS20(図9、図11参照)では、ステップS19において生成したブロックキーKb1を適用したAES復号処理を実行する。ステップS20では、ブロックキーKb1を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭TSパケット422の少なくともシード情報(シード2)を含むデータ領域がブロックキーKb1を適用した暗号処理のなされたデータ部である。従って、このシード情報(シード2)を含むデータ領域を対象としてブロックキーKb1を適用した復号処理を実行する。

30

【0130】

なお、ブロックキーKb1を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

【0131】

先頭TSパケット422には、他のユーザデータ部、すなわち、後続の5952バイトのTSパケット群423の復号処理に適用するブロックキーKb2を算出するために必要となるシード情報(シード2)432が含まれている。すなわち、シード情報(シード2)432は、ブロックキーKb1を適用した暗号処理がなされた暗号化データとして先頭TSパケット422に記録されている。

40

【0132】

ステップS20における、ブロックキーKb1を適用した復号処理の結果として、復号TSパケット424が算出され、その中からシード情報(シード2)を抽出する。

【0133】

図9のセレクトステップS21は、ブロックキーKb1を適用した復号処理の結果から、シード情報(シード2)をステップS22のブロックキーKb2生成ステップに出力し、ブロックキーKb2で暗号化された暗号化データを復号ステップS23に出力し、その他の復号データ(非暗号化データ)をセレクトステップS24に出力することを示している

50

。

【0134】

ステップS22（図9，図11参照）では、ステップS20におけるブロックキーKb1を適用した復号処理の結果取得された復号TSパケット424から抽出したシード情報（シード2）と、ステップS17（図9参照）において生成した記録キーK2とに基づいて、AES暗号処理を実行し、ブロックキーKb2を算出する。

【0135】

次に、ステップS23において、ブロックキーKb2を適用してユーザデータ部の暗号化部（ブロックキーKb2で暗号化されたデータ領域423）を復号し、復号TSパケット群425を生成する。

10

【0136】

復号TSパケット群425、および復号TSパケット426（=TSパケット424）は、セレクトステップS24において結合されて、復号TSパケットからなるコンテンツ412として再生制御処理手段255に入力される。

【0137】

再生制御処理手段255における再生制御処理について、図12を参照して説明する。再生制御処理手段255は、暗号処理手段250から、第2タイトルキー（Kt2）、411と、復号コンテンツ412を受領する。

【0138】

まず、再生制御処理手段255は、ステップS31において、情報記録媒体100に格納された暗号化ASCすなわち、第2タイトルキー（Kt2）で暗号化した編集スタジオコード（ASC：Authoring Studio Code）であるデータeKt2（ASC）を読み出し、暗号処理手段250から受信した第2タイトルキー（Kt2）を適用して復号処理を実行し、編集スタジオコード（ASC）を取得しメモリに格納する。

20

【0139】

さらに、再生制御処理手段255は、ステップS32において、情報記録媒体100に格納された暗号化DMCすなわち、第2タイトルキー（Kt2）で暗号化した情報記録媒体製造者コード（DMC：Disc Manufacturer Code）であるデータeKt2（DMC）を読み出し、暗号処理手段250から受信した第2タイトルキー（Kt2）を適用して復号処理を実行し、情報記録媒体製造者コード（DMC）を取得しメモリに格納する。

30

【0140】

再生制御処理手段255は、暗号処理手段250から受信した復号コンテンツ412から、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とを含むプログラムマップテーブルPMT（Program Map Table）を検出する。PMTは編集スタジオコード（ASC）と、情報記録媒体製造者コード（DMC）を含む情報であり、コンテンツ編集エンティティ330においてコンテンツに対して埋め込まれる。ステップS33において編集スタジオコード（ASC）検出、ステップS34において情報記録媒体製造者コード（DMC）検出を実行する。

【0141】

ステップS35において、PMTから検出した編集スタジオコード（ASC）と、ステップS31で、暗号化編集スタジオコードeKt2（ASC）の復号処理によって取得しメモリに格納した編集スタジオコード（ASC）との比較処理を実行する。

40

【0142】

さらに、ステップS36において、PMTから検出した情報記録媒体製造者コード（DMC）と、ステップS32で、暗号化情報記録媒体製造者コード（DMC）eKt2（DMC）の復号処理によって取得しメモリに格納した情報記録媒体製造者コード（DMC）との比較処理を実行する。

【0143】

さらに、ステップS37において、コンテンツ412中から、編集スタジオコード（AS

50

C)と情報記録媒体製造者コード(DMC)を含む電子透かしが規定時間内に検出され、電子透かし格納情報と、メモリ格納情報とが一致したか否かを判定する。再生制御処理手段255では、コンテンツの再生開始からタイマを設定し、予め定めた定時間内に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を含む電子透かしが検出されたか否かを判定する。

【0144】

ステップS38において、ステップS35における比較結果の一致、すなわち、PMTから検出した編集スタジオコード(ASC)と、メモリに格納した編集スタジオコード(ASC)との一致、ステップS36における比較結果の一致、すなわち、PMTから検出した情報記録媒体製造者コード(DMC)と、メモリに格納した情報記録媒体製造者コード(DMC)との一致、さらに、ステップS37における規定時間内の電子透かし検出、照合のすべてを満足したか否かを判定する。

10

【0145】

ステップS39において、ステップS38の判定がYesであればコンテンツ再生を継続し、Noであれば、コンテンツ再生を停止する。

【0146】

図13、図14を参照してコンテンツ再生を実行するユーザデバイスとしての情報処理装置におけるコンテンツ再生処理手順の一連の処理について説明する。

【0147】

ステップS101において、情報処理装置(ユーザデバイス)は、情報記録媒体から暗号鍵情報および識別情報の読み取りを実行する。ステップS102において、読み取り情報および自デバイスに格納したデバイスキーに基づいてタイトルキー(Kt1, Kt2)を生成する。

20

【0148】

ステップS103において、情報記録媒体からディスクID(S, Sig)を読み取り、検証処理を実行する。検証が成立しない場合は、この時点でコンテンツ再生は停止する。検証が成立すると、ステップS105において、記録キーK1, K2を生成する。

【0149】

ステップS106において、第2タイトルキー(Kt2)に基づいて情報記録媒体から読み出した暗号化ASC、暗号化DMC、すなわち、eKt2(ASC)、eKt2(DMC)の復号処理を実行して、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)をメモリに格納する。

30

【0150】

ステップS107において、ブロックキーKb1, Kb2を生成し、生成したブロックキーKb1, Kb2に基づくコンテンツの復号、再生処理を開始する。

【0151】

ステップS108では、コンテンツ再生を実行しながらPMTおよび電子透かしの検出処理を実行する。ステップS109においてPMTから編集スタジオコード(ASC)が検出されるとステップS110において検出した編集スタジオコード(ASC)と、メモリに格納済みの編集スタジオコード(ASC)との比較処理を実行し、一致しなかった場合は、ステップS121でコンテンツ再生を停止する。

40

【0152】

一致した場合は、さらに、ステップS111に進み、PMTから情報記録媒体製造者コード(DMC)が検出されると、ステップS112において検出した情報記録媒体製造者コード(DMC)と、メモリに格納済みの情報記録媒体製造者コード(DMC)との比較処理を実行し、一致しなかった場合は、ステップS121でコンテンツ再生を停止する。

【0153】

一致した場合は、さらに、ステップS113に進み、電子透かし情報から編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)が検出されると、ステップS114において検出した編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC

50

）と、メモリに格納済みの編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）との比較処理を実行し、一致しなかった場合は、ステップS121でコンテンツ再生を停止する。

【0154】

ステップS115では、予め定めた時間内に、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とのPMTと電子透かし情報が検出されたか否かが判定され、検出されなかった場合は、ステップS121でコンテンツ再生を停止する。

【0155】

編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とのPMT、電子透かし情報との検出処理は規定時間毎に繰り返し実行する。

10

【0156】

このようにして、暗号化コンテンツの復号およびコンテンツ再生制御が実行されることになる。なお、図14のフローでは、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とのPMT、電子透かし情報との検出処理を繰り返し実行する処理として説明したが、1つの編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とのPMT、電子透かし情報との検出がなされ、両者がメモリ格納情報と一致した場合は、その後の電子透かし検出処理を実行しない構成としてもよい。

【0157】

上述したように、情報記録媒体に格納されたコンテンツは、シード情報（シード1）およびシード情報（シード2）によって生成されるブロック鍵Kb1、Kb2で暗号化され、シード情報（シード2）は、シード情報（シード1）を用いて生成される鍵、すなわちブロックキーKb1によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード2）の解析、シード情報（シード2）を適用して生成するブロックキーKb2の解析、ブロックキーKb2によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

20

【0158】

さらに、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

30

【0159】

次に、図15、図16、図17を参照してシード情報（シード1）と記録キーKに基づいて生成するブロックキーKb1によって暗号化する領域の例について説明する。図15は、制御ブロックにシード情報（シード1）が格納され、シード情報（シード2）が、ユーザデータの1つのTSパケットに含まれる場合の例である。先に図11を参照して説明した例では、シード情報（シード2）が、ユーザデータの先頭または2番目のTSパケット内に含まれる場合について説明したが、シード情報（シード2）は、先頭、または第2番目のTSパケット以外のユーザデータ部を構成する任意のTSパケット内に格納可能である。

40

【0160】

ユーザデータのいずれかのTSパケットにシード情報（シード2）を格納した場合、シード情報（シード1）と記録キーK1とに基づいて生成するブロックキーKb1によって暗号化する領域例として、例えば図15（a）～（c）の構成がある。（a）は、シード情報（シード2）のみをブロックキーKb1によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード2）と記録キーK2によって生成されるブロックキーKb2によって暗号化したデータ領域とする。

50

【0161】

(b) は、シード情報 (シード2) を含む TS パケットの一部領域をブロックキー K b 1 によって暗号化した例である。

【0162】

(c) は、シード情報 (シード2) を含む 1 つの TS パケットの全領域をブロックキー K b 1 によって暗号化した例である。

【0163】

図 16 に示す例は、シード情報 (シード1) とシード情報 (シード2) を同一の TS パケット内に格納した例を示している。シード情報 (シード1) は非暗号化情報として格納される。シード情報 (シード2) は、シード情報 (シード1) と記録キー K 1 とに基づいて生成するブロックキー K b 1 によって暗号化され、シード情報 (シード1) と同一の TS パケット内に格納される。

10

【0164】

(d) は、シード情報 (シード2) のみをブロックキー K b 1 によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報 (シード2) と記録キー K 2 によって生成されるブロックキー K b 2 によって暗号化したデータ領域とする。

【0165】

(e) は、シード情報 (シード2) を含む TS パケットの一部領域をブロックキー K b 1 によって暗号化した例である。(f) は、シード情報 (シード2) を含む 1 つの TS パケットの全領域をブロックキー K b 1 によって暗号化した例である。

20

【0166】

図 17 に示す例は、シード情報 (シード1) とシード情報 (シード2) を異なる TS パケット内に格納した例を示している。シード情報 (シード1) は非暗号化情報として格納される。シード情報 (シード2) は、シード情報 (シード1) と記録キー K 1 とに基づいて生成するブロックキー K b 1 によって暗号化され、シード情報 (シード1) と異なる TS パケット内に格納される。

【0167】

(g) は、シード情報 (シード2) のみをブロックキー K b 1 によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報 (シード2) と記録キー K 2 によって生成されるブロックキー K b 2 によって暗号化したデータ領域とする。

30

【0168】

(h) は、シード情報 (シード2) を含む TS パケットの一部領域をブロックキー K b 1 によって暗号化した例である。(i) は、シード情報 (シード2) を含む 1 つの TS パケットの全領域をブロックキー K b 1 によって暗号化した例である。

【0169】

以上、図 15 ～ 図 17 を参照して説明したように、シード情報 (シード1) およびシード情報 (シード2) の格納態様、および暗号化データ領域の設定態様は様々な設定が可能である。しかし、いずれの場合もシード情報 (シード2) は、シード情報 (シード1) を用いて生成される鍵、すなわちブロックキー K b 1 によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報 (シード2) の解析、シード情報 (シード2) を適用して生成するブロックキー K b 2 の解析、ブロックキー K b 2 によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

40

【0170】

[情報記録媒体に対するデータ格納処理]

先に図 2 を参照して説明したように、暗号化コンテンツを格納した情報記録媒体は、コンテンツ編集エンティティ (AS: Authoring Studio) 330 において編集され、その後、情報記録媒体製造エンティティ (DM: Disc Manufactu

50

rer) 350において、ユーザに提供される媒体としてのCD、DVD等が大量に複製(レプリカ)されて、情報記録媒体100が製造され、ユーザに提供される。

【0171】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ(TC:Trusted Center)300である。管理センタ(TC:Trusted Center)300は、コンテンツ編集エンティティ(AS:Authoring Studio)330、および情報記録媒体製造エンティティ(DM:Disc Manufacturer)350に対して様々な管理情報を提供し、コンテンツ編集エンティティ(AS:Authoring Studio)330、および情報記録媒体製造エンティティ(DM:Disc Manufacturer)350は、管理センタ(TC:Trusted Center)300から受領した管理情報に基づいて、コンテンツ編集、暗号化、鍵情報の、生成、格納処理などを行う。

10

【0172】

管理センタ300、コンテンツ編集エンティティ330、および情報記録媒体製造エンティティ350の実行する処理の詳細について、図18以下を参照して説明する。

【0173】

図18には、管理センタ300、コンテンツ編集エンティティ330、および情報記録媒体製造エンティティ350の実行する処理を示している。

【0174】

管理センタ300は、コンテンツ保持者からのコンテンツ501を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキーKm502、第2タイトルキーKt2、503、第1タイトルキーKt1、504、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506、ディスク固有シードS507、製造を許容する情報記録媒体の数、量産発注枚数N508を設定する。

20

【0175】

管理センタ300は、コンテンツ保持者からのコンテンツ501に対して、ステップS41において、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506を電子透かしとして埋め込む。

【0176】

ステップS42では、ディスク固有シードS507に基づいて、ディスク固有キーKd511を生成する。

30

【0177】

管理センタ300は、電子透かしを埋め込んだコンテンツと、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506、および、ディスク固有シードS507に基づいて生成したディスク固有キーKd511をコンテンツ編集エンティティ330に提供する。

【0178】

さらに、管理センタ300は、ステップS43において、メディアキーKm502をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしてのEKB512を生成する。

40

【0179】

ステップS44では、メディアキーKm502に基づいて第2タイトルキーKt2、503を暗号化して暗号化第2タイトルキーeKm(Kt2)513を生成し、ステップS45では、メディアキーKm502に基づいて第1タイトルキーKt1、504を暗号化して暗号化第1タイトルキーeKm(Kt1)514を生成する。

【0180】

さらに、ステップS46において、編集スタジオコード(ASC)505を第2タイトルキーKt2、503で暗号化し、暗号化ASCであるeKt2(ASC)515を生成し、ステップS47において、情報記録媒体製造者コード(DMC)506を第2タイトル

50

キー K_{t2} 、503で暗号化し、暗号化DMCである $eK_{t2}(DMC)$ 516を生成する。

【0181】

さらに、ディスク固有シード S_{507} に対応して、製造を許容する情報記録媒体の数、量産発注枚数 N_{508} に基づく N 個の (S, Sig) 、すなわち N 個の個別ディスク ID_{517} を生成する。

【0182】

EKB_{512} 、暗号化第2タイトルキー $eK_m(K_{t2})_{513}$ 、暗号化第1タイトルキー $eK_m(K_{t1})_{514}$ 、暗号化ASCである $eK_{t2}(ASC)_{515}$ 、暗号化DMCである $eK_{t2}(DMC)_{516}$ 、 N 個の個別ディスク ID_{517} と第1タイトルキー K_{t1} は、管理センタ300から、情報記録媒体製造エンティティ350に提供される。

10

【0183】

次に、コンテンツ編集エンティティ330の処理について説明する。コンテンツ編集エンティティ330は、管理センタ300から受領した電子透かし埋め込み済みのコンテンツの符号化、例えばMPEG符号化処理をエンコーダ531において実行し、トランスポートストリームデータを生成し、さらに、管理センタ300から受領した編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)の埋め込み処理をPMT(Program Map Table)埋め込み部532において実行する。PMTは編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)を含む情報であり、コンテンツ編集エンティティ330においてコンテンツに対して埋め込まれる。

20

【0184】

次に暗号処理部533において暗号処理が実行される。コンテンツ編集エンティティ330の暗号処理部533における処理の詳細について、図19を参照して説明する。

【0185】

コンテンツ編集エンティティ330は、ステップS51において乱数に基づいて記録シード(REC SEED)を生成する。記録シード(REC SEED)は出力データとして、情報記録媒体製造エンティティに渡されるデータである。さらに、ステップS52において、管理センタ300から受領したディスク固有キー K_d と、記録シード(REC SEED)を適用した暗号処理により、記録キー K_2 を生成し、ステップS53において、コンテンツ中から選択したシード情報(シード2)と記録キー K_2 とに基づいてブロックキー K_{b2} を生成(ステップS54)し、ステップS55において、ブロックキー K_{b2} に基づいて、コンテンツの暗号化処理を実行する。セクタステップS53ではシード2を選択するとともに、ステップS55における暗号処理を実行するデータ部と、ステップS55における暗号処理を実行しないデータ部が分離され、ステップS56において暗号処理データと非暗号処理データとが再度結合されて出力データとして、記録シード(REC SEED)とともにディスクイメージデータとして情報記録媒体製造エンティティに渡される。

30

【0186】

コンテンツ編集エンティティ330の出力するデータは、図19(b)に示すように、シード情報(シード2)が平文データとして設定され、その他がシード2を適用して生成されるブロック鍵 K_{b2} によって暗号化され、この暗号化データ中には、編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)とを含むPMT(Program Map Table)が格納されている。

40

【0187】

次に、図18に戻り、情報記録媒体製造エンティティ350の処理について説明する。情報記録媒体製造エンティティ350は、コンテンツ編集エンティティ350からの受領コンテンツに対して、まず、暗号処理部551において暗号処理を実行する。

【0188】

情報記録媒体製造エンティティ350の暗号処理部551において実行する暗号処理の詳細について図20を参照して説明する。

50

【0189】

情報記録媒体製造エンティティ350は、ステップS61において乱数に基づいて物理インデックスを生成する。さらに、ステップS62において、管理センタ300から受領した第1タイトルキーKt1と、物理インデックスを適用した暗号処理により、記録キーK1を生成し、ステップS63において、コンテンツ中から選択したシード情報（シード1）と記録キーK1とに基づいてブロックキーKb1を生成（ステップS64）し、ステップS65において、ブロックキーKb1に基づいて、コンテンツ中のシード情報（シード2）を含むデータ領域の暗号化処理を実行する。セレクトステップS63ではシード1を選択するとともに、ステップS65における暗号処理を実行するデータ部と、ステップS65における暗号処理を実行しないデータ部が分離され、ステップS66において暗号処理データと非暗号処理データとが再度結合されて出力データとされる。 10

【0190】

情報記録媒体製造エンティティ350の暗号処理部551の出力するデータは、図20（b）に示すように、シード情報（シード1）が平文データとして制御データ（UCD: User control Data）中に設定され、シード2を含むデータ領域がシード1を適用して生成されるブロック鍵Kb1によって暗号化されたデータとなる。

【0191】

図18に戻り、情報記録媒体製造エンティティ350の処理について説明を続ける。情報記録媒体製造エンティティ350の暗号処理部551の出力データは、フォーマット処理部552に入力され、管理センタ300から受領するEKB512、暗号化第2タイトルキーeKm（Kt2）513、暗号化第1タイトルキーeKm（Kt1）514、暗号化ASCであるeKt2（ASC）515、暗号化DMCであるeKt2（DMC）516をディスクのリードイン領域（図1参照）に書き込む処理を実行する。その書き込み処理の際に、図20（a）ステップS61において生成された物理インデックスが同時に情報記録媒体に記録される。 20

【0192】

さらに、これらの情報を有する情報記録媒体（ディスク）のレプリカを複製製造部553において製造する。製造数は、管理センタ300の設定した量産発注枚数Nに対応する数であり、各情報記録媒体毎に管理センタ300から受領した異なるディスクIDが格納される。 30

【0193】

これらの全情報の格納処理がなされると、情報記録媒体100が市場に流通し、ユーザに提供されユーザの情報処理装置において、前述した復号処理および再生制御処理に基づいてコンテンツ再生が実行される。情報記録媒体100は、図1を参照して説明した各種の情報を格納し、ユーザの情報処理装置において、図8～図14を参照して説明した復号、制御に基づく再生が実行される。

【0194】

〔ディスクIDを用いない処理構成〕

上述した実施例では、情報記録媒体に各媒体毎に異なるディスクIDを設定し、ユーザデバイス側でディスクIDを情報記録媒体から取得し、検証の後、ディスクIDの構成要素としてのディスク固有シードSを適用してディスク固有キーKdを生成（図9ステップS15）し、ディスク固有キーKdを適用したコンテンツ復号を実行する構成を説明した。 40

【0195】

しかし、情報記録媒体毎に異なるIDを記録する処理は手間がかかる処理であり、大量のディスクを量産する場合には、省略したい場合もある。以下、情報記録媒体毎に異なるディスクIDを用いない処理例について説明する。

【0196】

図21に、管理センタ300、コンテンツ編集エンティティ330、および情報記録媒体製造エンティティ350の実行するディスクIDを用いない処理例を示している。

【0197】

図 21 において点線枠領域 600 の構成が、先に図 18 を参照して説明したディスク ID を適用した処理例と異なる部分である。なお、先に図 18 を参照して説明したディスク ID 関連の処理、構成は、図 21 には示されていない。

【0198】

管理センタ 300 は、コンテンツ保持者からのコンテンツ 501 を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキー Km 502、第 2 タイトルキー Kt 2, 503、第 1 タイトルキー Kt 1, 504、編集スタジオコード (ASC) 505、情報記録媒体製造者コード (DMC) 506、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応して設定される第 3 タイトルキー Kt 3, 601 を設定する。

10

【0199】

本例においては、図 18 を参照して説明したディスク固有シード S 507、製造を許容する情報記録媒体の数、すなわち量産発注枚数 N 508 が省略される。

【0200】

管理センタ 300 は、コンテンツ保持者からのコンテンツ 501 に対して、ステップ S 41 において、編集スタジオコード (ASC) 505、情報記録媒体製造者コード (DMC) 506 を電子透かしとして埋め込む。

【0201】

管理センタ 300 は、電子透かしを埋め込んだコンテンツと、編集スタジオコード (ASC) 505、情報記録媒体製造者コード (DMC) 506、および、ディスク固有キー (Disc Unique Key) Kd, 511 をコンテンツ編集エンティティ 330 に提供する。

20

【0202】

さらに、管理センタ 300 は、ステップ S 43 において、メディアキー Km 502 をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしての EKB 512 を生成する。

【0203】

ステップ S 44 では、メディアキー Km 502 に基づいて第 2 タイトルキー Kt 2, 503 を暗号化して暗号化第 2 タイトルキー eKm (Kt 2) 513 を生成し、ステップ S 45 では、メディアキー Km 502 に基づいて第 1 タイトルキー Kt 1, 504 を暗号化して暗号化第 1 タイトルキー eKm (Kt 1) 514 を生成する。

30

【0204】

さらに、ステップ S 46 において、編集スタジオコード (ASC) 505 を第 2 タイトルキー Kt 2, 503 で暗号化し、暗号化 ASC である eKt 2 (ASC) 515 を生成し、ステップ S 47 において、情報記録媒体製造者コード (DMC) 506 を第 2 タイトルキー Kt 2, 503 で暗号化し、暗号化 DMC である eKt 2 (DMC) 516 を生成する。

【0205】

さらに、ステップ S 71 において、第 3 タイトルキー Kt 3, 601 をメディアキー Km 502 に基づいて暗号化して暗号化第 3 タイトルキー eKm (Kt 3) 602 を生成する。

40

【0206】

EKB 512、暗号化第 2 タイトルキー eKm (Kt 2) 513、暗号化第 1 タイトルキー eKm (Kt 1) 514、暗号化 ASC である eKt 2 (ASC) 515、暗号化 DMC である eKt 2 (DMC) 516、暗号化第 3 タイトルキー eKm (Kt 3) 602 は、管理センタ 300 から、情報記録媒体製造エンティティ 350 に提供される。

【0207】

コンテンツ編集エンティティ 330 の処理、情報記録媒体製造エンティティ 350 の処理は、基本的に先に図 18～図 20 を参照して説明した処理と同様である。ただし、情報記録媒体製造エンティティ 350 のフォーマット処理部 552 は、情報記録媒体のリードイ

50

ン領域に書き込む処理を実行し、情報記録媒体製造エンティティ350の複製製造部553は、ディスク毎のディスクIDの書き込み処理を実行しない。

【0208】

この結果として製造される情報記録媒体100は、図22に示すようなデータを格納することになる。

【0209】

図22に示すように、情報記録媒体100には、物理インデックス102、暗号化コンテンツ103、記録シード(REC SEED)104、暗号鍵情報120が格納される。暗号鍵情報120は、情報記録媒体100のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域110に格納される。

10

【0210】

暗号鍵情報120には、暗号化第3タイトルキーeKm(Kt3)が含まれる。図1の構成と異なる点は、ディスクIDが格納されない点と、暗号鍵情報120に暗号化第3タイトルキーeKm(Kt3)611が追加された点である。

【0211】

この情報記録媒体を再生する情報処理装置(ユーザデバイス)の暗号処理手段の実行するコンテンツ復号処理について図23を参照して説明する。

【0212】

図23の処理中、先に図9を参照して説明したディスクIDを持つ情報記録媒体の再生処理と異なる点は、情報記録媒体100が、暗号化第3タイトルキーeKm(Kt3)611を持つ点、ステップS82のディスク固有キーKdの生成処理、ステップS81の暗号化第3タイトルキーeKm(Kt3)611の復号処理である。

20

【0213】

本実施例においては、ディスク固有キーKdの生成処理をディスクIDから取得したディスク固有シードS(図9、ステップS14参照)を適用しない。

【0214】

本実施例では、ステップS81において、暗号化第3タイトルキーeKm(Kt3)611をメディアキーKmを用いて復号して、第3タイトルキーKt3を取得し、取得した第3タイトルキーKt3と、ステップS12の復号処理で取得した第2タイトルキーKt2に基づく暗号処理をステップS82において実行してディスク固有キーKdの生成処理を実行する構成としている。

30

【0215】

以下の処理は、先に図9を参照して説明した処理と同様である。本処理例においては、ディスクIDを用いない構成であるので、情報記録媒体毎に異なるIDを記録する処理が不要となり、大量のディスクを量産する場合等、情報記録媒体製造エンティティの処理が軽減される。

【0216】

本例においても、情報記録媒体に格納されたコンテンツは、シード情報(シード1)およびシード情報(シード2)によって生成されるブロック鍵Kb1、Kb2で暗号化され、シード情報(シード2)は、シード情報(シード1)を用いて生成される鍵、すなわちブロックキーKb1によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報(シード2)の解析、シード情報(シード2)を適用して生成するブロックキーKb2の解析、ブロックキーKb2によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

40

【0217】

さらに、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)の検出、照合一致を条件として再生処理を実行する構成としたので、不正なコードあるいは電子透かしを持たないコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となり、また不正な複製が製造され、流通した場合において、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を検出

50

することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【0218】

[情報処理装置他のエンティティ構成例]

次に、上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティティ、情報記録媒体製造エンティティ、各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例を図24を参照して説明する。上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティティ、情報記録媒体製造エンティティ、各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置としては、例えばPC、情報処理サーバ等の汎用的な情報処理装置が適用可能である。以下、図24を参照して、上述した各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例について説明する。

10

【0219】

CPU (Central Processing Unit) 701は、ROM (Read Only Memory) 702に記憶されている各種プログラム、あるいは、記憶部708に格納され、RAM (Random Access Memory) 703にロードされたプログラムに従って各種処理を実行する。タイマ700は計時処理を行ない、クロック情報をCPU 701に供給する。

【0220】

ROM (Read Only Memory) 702は、CPU 701が使用するプログラムや演算用のパラメータ、固定データ等を格納する。RAM (Random Access Memory) 703は、CPU 701の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はバス711により相互に接続されている。

20

【0221】

暗号処理部704は、上述した各種の暗号処理、例えばAES暗号化アルゴリズムを適用した暗号処理等を実行する。WM処理部713は、例えばスペクトラム拡散技術を用いて、データを不可視な情報としてビデオ信号へ埋め込む、あるいはデータを認識できない情報としてオーディオ信号へ埋め込む、などインフォメーションハイディング (Information Hiding) 技術に基づく処理を実行する。

30

【0222】

入出力インタフェース712には、キーボード、マウス等の入力部706、CRT、LCD等のディスプレイ、スピーカ等からなる出力部707、ハードディスク等の記憶部708、通信部709が接続される。通信部709は、例えばインターネット等の通信網を介したデータ送受信により、たとえば各エンティティ間の通信を行なう。

【0223】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

40

【0224】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0225】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブル

50

ディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0226】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

10

【0227】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0228】

【発明の効果】

以上、説明したように、本発明の構成によれば、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

20

【0229】

さらに、本発明の構成によれば、情報記録媒体に格納されたコンテンツは、シード情報 (シード1) およびシード情報 (シード2) によって生成されるブロック鍵 Kb1、Kb2 で暗号化され、シード情報 (シード2) は、シード情報 (シード1) を用いて生成される鍵、すなわちブロックキー Kb1 によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報 (シード2) の解析、シード情報 (シード2) を適用して生成するブロックキー Kb2 の解析、ブロックキー Kb2 によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

30

【0230】

さらに、本発明の構成によれば、コンテンツ編集エンティティが、鍵生成情報としての記録シード (RECS EED) を生成し、管理センタから受領する鍵情報、および鍵生成情報 (第2シード) とに基づいて第2ブロックキー Kb2 を生成し、第2ブロックキー Kb2 に基づくコンテンツ暗号化を実行し、情報記録媒体製造エンティティが、鍵生成情報としての物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報 (第1シード) に基づいてブロックキー Kb1 を生成し、生成した第1ブロックキー Kb1 に基づく第2シードの暗号化を実行する構成とし、さらに、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製された場合には、コード検出による情報漏洩ルートの解析が可能となる。

40

【図面の簡単な説明】

【図1】 情報記録媒体に格納されるデータ構成について説明する図である。

【図2】 情報記録媒体に格納されるデータの管理、情報記録媒体の製造ルートについて説明する図である。

50

【図 3】各種キー、データの暗号化処理、配布処理に適用される階層型木構造を説明する図である。

【図 4】各種キー、データの配布に使用される有効化キーブロック（E K B）の例を示す図である。

【図 5】コンテンツ鍵の有効化キーブロック（E K B）を使用した配布例と復号処理例を示す図である。

【図 6】情報記録媒体に格納されるデータ構成について説明する図である。

【図 7】情報処理装置の構成例について説明する図である。

【図 8】情報処理装置において実行するコンテンツ復号、再生制御処理について説明する図である。

10

【図 9】情報処理装置において実行するコンテンツ復号処理について説明する図である。

【図 10】ディスク固有キーの生成処理例について説明する図である。

【図 11】暗号化データの復号処理シーケンスを説明する図である。

【図 12】コンテンツの再生制御処理について説明する図である。

【図 13】コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。

【図 14】コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。

【図 15】シード情報の格納構成例について説明する図である。

【図 16】シード情報の格納構成例について説明する図である。

20

【図 17】シード情報の格納構成例について説明する図である。

【図 18】各エンティティ毎の情報記録媒体に対して実行するデータ格納、暗号化処理を説明する図である。

【図 19】コンテンツ編集エンティティの実行する暗号処理を説明する図である。

【図 20】情報記録媒体製造エンティティの実行する暗号処理を説明する図である。

【図 21】ディスク I D を用いない処理例における各エンティティ毎の情報記録媒体に対して実行するデータ格納、暗号化処理を説明する図である。

【図 22】ディスク I D を用いない処理例における情報記録媒体に格納されるデータ構成について説明する図である。

【図 23】ディスク I D を用いない処理例における情報処理装置において実行するコンテンツ復号処理について説明する図である。

30

【図 24】ユーザデバイス、各エンティティにおいて適用する情報処理装置の構成例を示す図である。

【符号の説明】

- 100 情報記録媒体
- 101 ディスク I D
- 102 物理インデックス
- 103 暗号化コンテンツ
- 104 記録シード
- 110 リードイン領域
- 120 暗号鍵情報
- 121 E K B
- 122 暗号化第 1 タイトルキー e K m (K t 1)
- 123 暗号化第 2 タイトルキー e K m (K t 2)
- 124 暗号化 A S C , e K t 2 (A S C)
- 125 暗号化 D M C : e K t 2 (D M C)
- 200 情報処理装置
- 300 管理センタ
- 330 コンテンツ編集エンティティ
- 350 情報記録媒体製造エンティティ

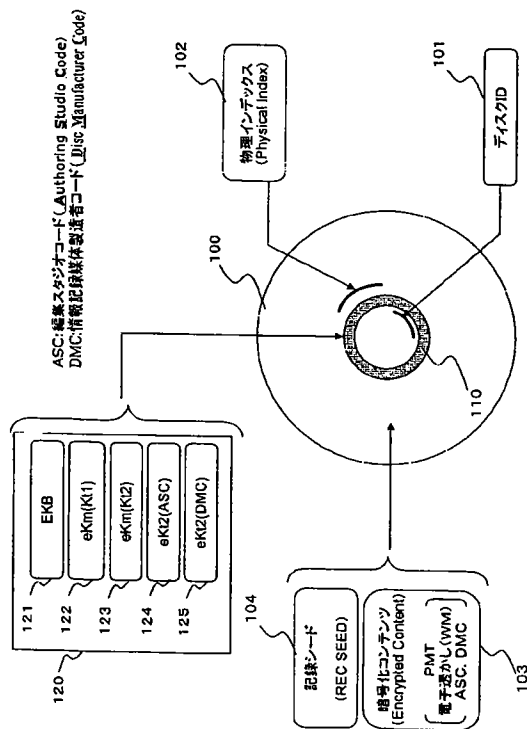
40

50

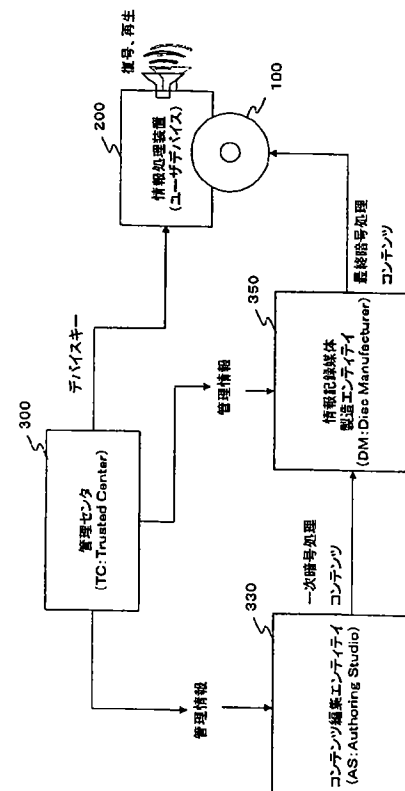
2 1 0	バス	
2 2 0	入出力インタフェース	
2 3 0	M P E G コーデック	
2 4 0	入出力インタフェース	
2 4 1	A / D , D / A コンバータ	
2 5 0	暗号処理手段	
2 5 5	再生制御処理手段	
2 6 0	R O M	
2 7 0	R A M	
2 8 0	メモリ	10
2 9 0	記録媒体 I / F	
2 9 5	記録媒体	
2 9 8	T S 処理手段	
4 0 1	E K B	
4 0 2	暗号化第 2 タイトルキー e K m (K t 2)	
4 0 3	暗号化第 1 タイトルキー e K m (K t 1)	
4 0 4	ディスク I D	
4 0 5	記録シード	
4 0 6	物理インデックス	
4 0 7	暗号化コンテンツ	20
4 1 0	デバイスキー	
4 1 1	第 2 タイトルキー K t 2	
4 1 2	コンテンツ	
4 2 0	暗号処理単位	
4 2 1	制御データ	
4 2 2	先頭 T S パケット	
4 2 3	後続 T S パケット	
4 2 4	復号 T S パケット	
4 2 5	復号 T S パケット群	
4 2 6	復号 T S パケット	30
4 3 1	シード情報 (シード 1)	
4 3 2	シード情報 (シード 2)	
5 0 1	コンテンツ	
5 0 2	メディアキー	
5 0 3	第 1 タイトルキー	
5 0 4	第 2 タイトルキー	
5 0 5	コンテンツ編集エンティティコード (A S C : A u t h o r i n g S t u d i o C o d e)	
5 0 6	情報記録媒体製造者コード (D M C : D i s c M a n u f a c t u r e r C o d e)	40
5 0 7	ディスク固有シード S	
5 0 8	量産発注コード	
5 1 1	ディスク固有キー K d	
5 1 2	E K B	
5 1 3	暗号化第 2 タイトルキー e K m (K t 2)	
5 1 4	暗号化第 1 タイトルキー e K m (K t 1)	
5 1 5	暗号化 A S C , e K t 2 (A S C)	
5 1 6	暗号化 D M C : e K t 2 (D M C)	
5 1 7	個別ディスク I D	
5 3 1	エンコーダ	50

5 3 2	P M T 埋め込み部	
5 3 3	暗号処理部	
5 5 1	暗号処理部	
5 5 2	フォーマット処理部	
5 5 3	複製製造部	
6 0 1	第3タイトルキー $K_t 3$	
6 0 2	暗号化第3タイトルキー $e K_m (K_t 1)$	
6 1 1	暗号化第3タイトルキー $e K_m (K_t 1)$	
7 0 0	タイマ	
7 0 1	C P U (C e n t r a l p r o c e s s i n g U n i t)	10
7 0 2	R O M (R e a d - O n l y - M e m o r y)	
7 0 3	R A M (R a n d o m A c c e s s M e m o r y)	
7 0 4	暗号処理部	
7 0 6	入力部	
7 0 7	出力部	
7 0 8	記憶部	
7 0 9	通信部	
7 1 0	ドライブ	
7 1 1	バス	
7 1 2	入出力インタフェース	
7 1 3	W M (W a t e r m a r k) 処理部	20
7 2 1	リムーバブル記録媒体	

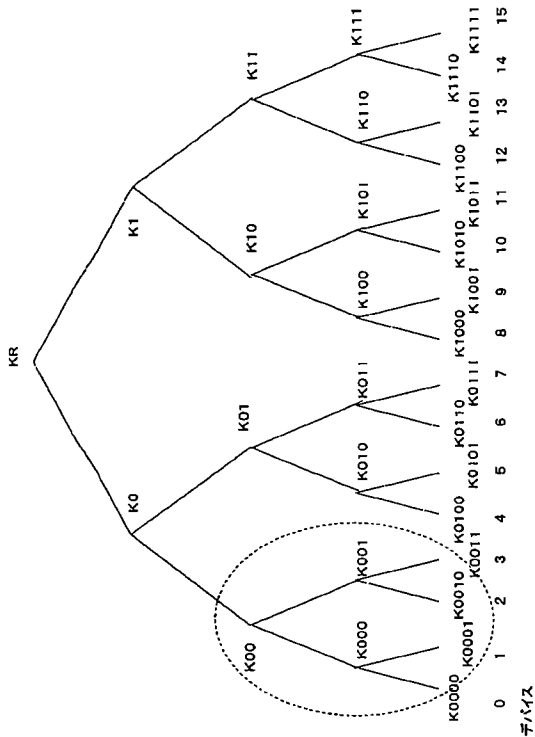
【図 1】



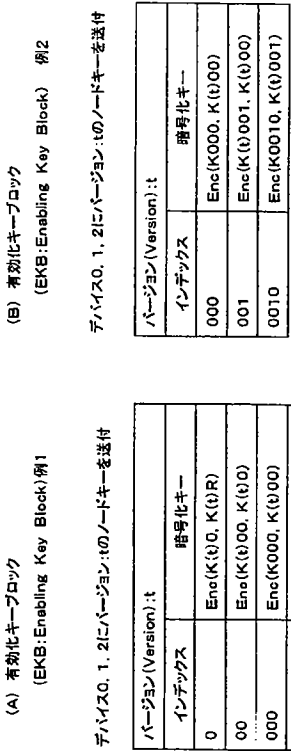
【図 2】



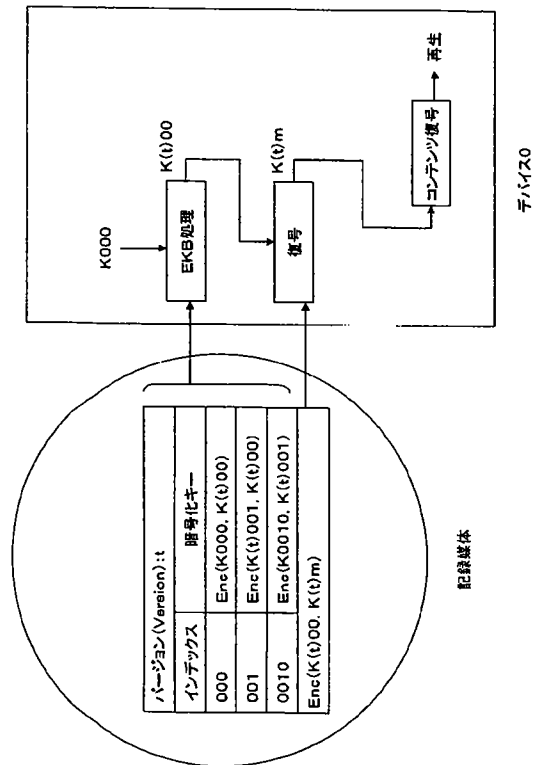
【図 3】



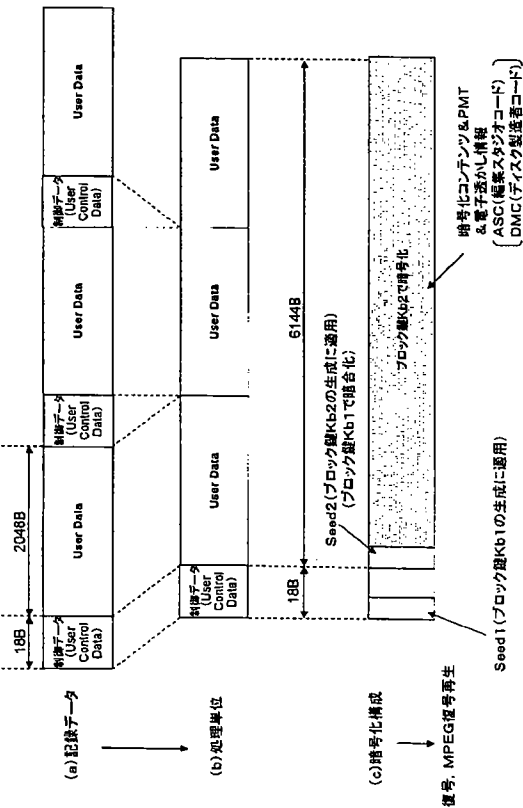
【図 4】



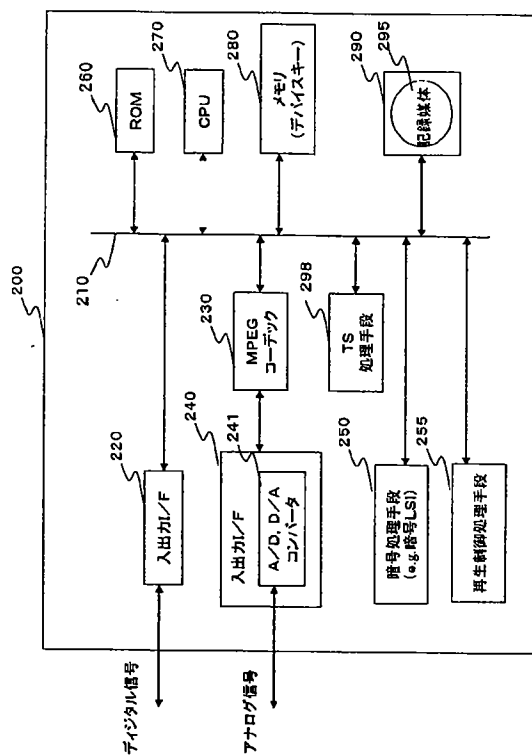
【図 5】



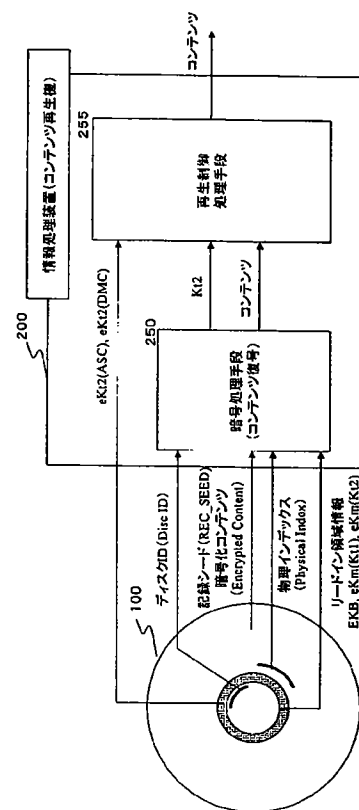
【図 6】



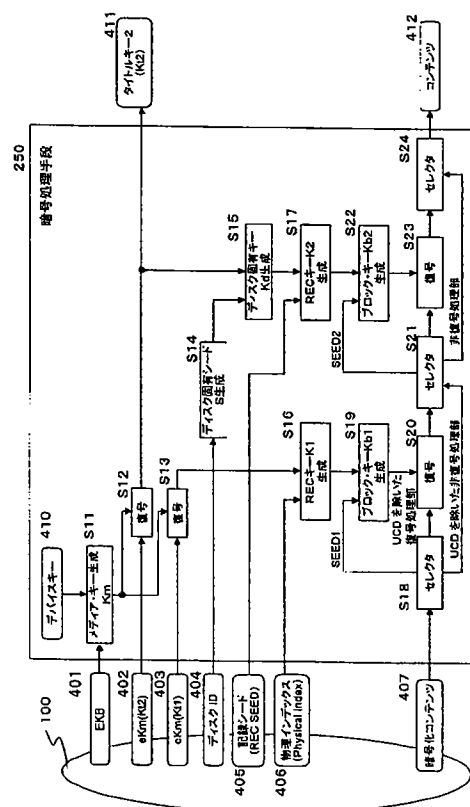
【图 7】



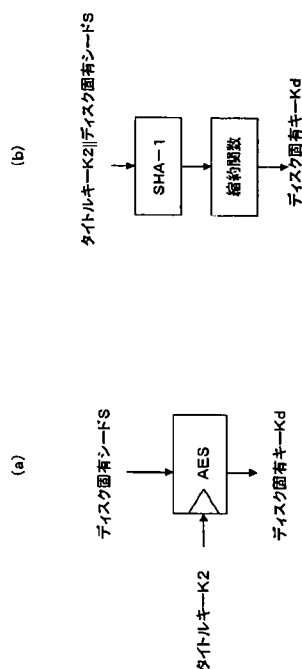
【图 8】



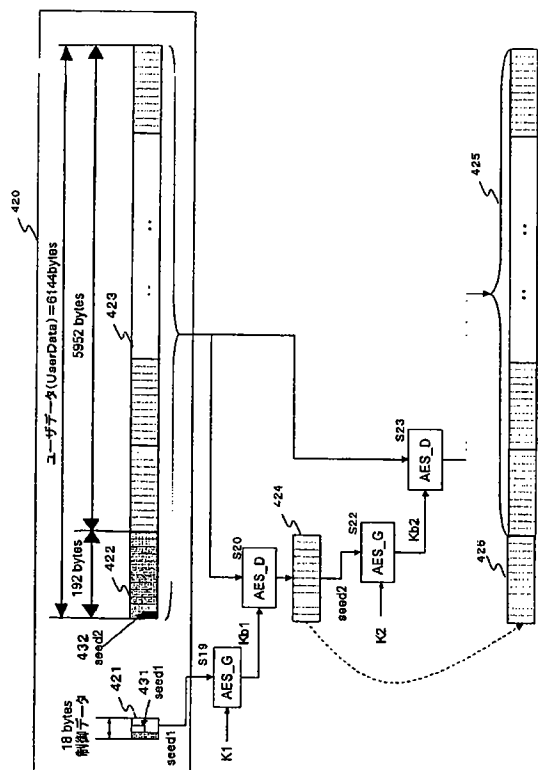
【図 9】



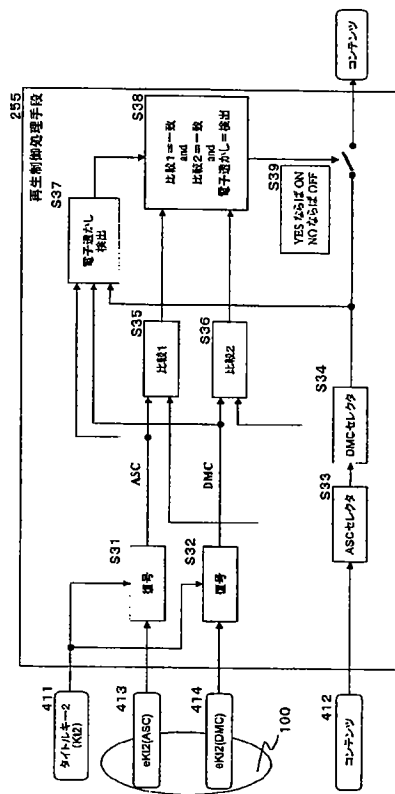
【図 10】



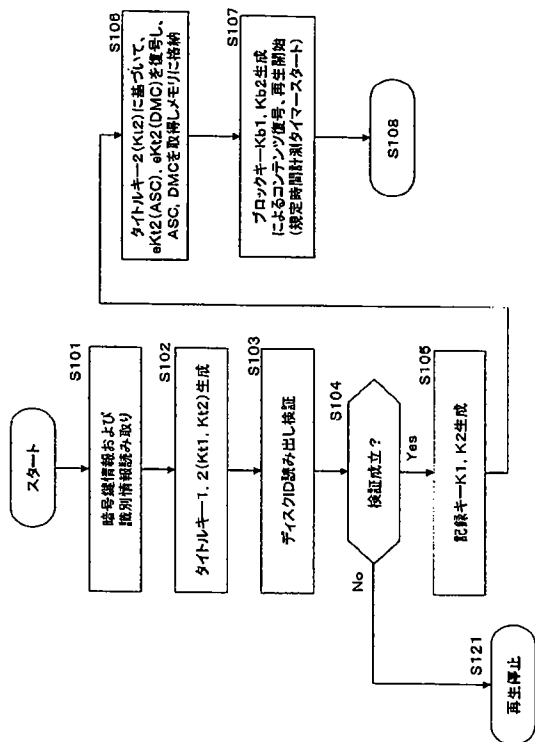
【図11】



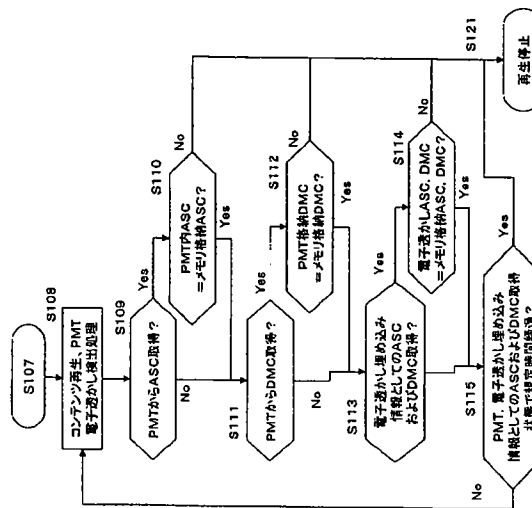
【図12】



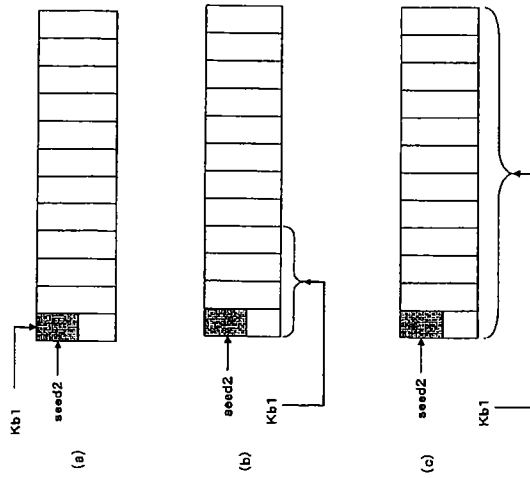
【図13】



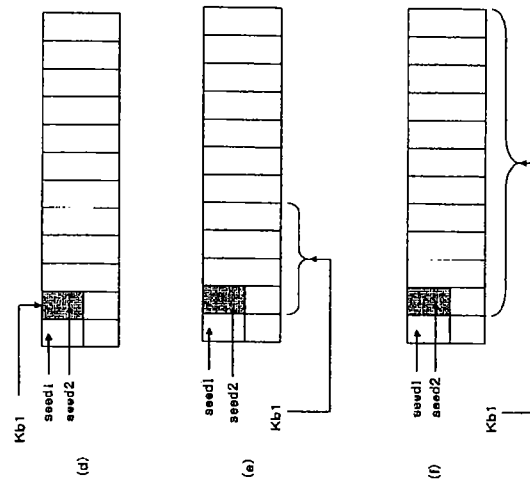
【図14】



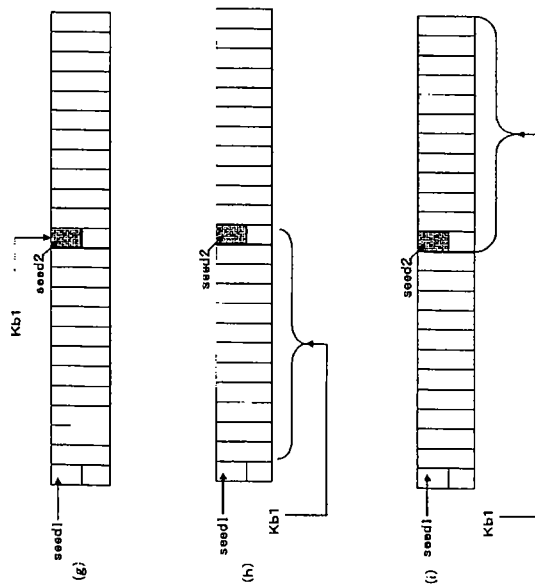
【图 15】



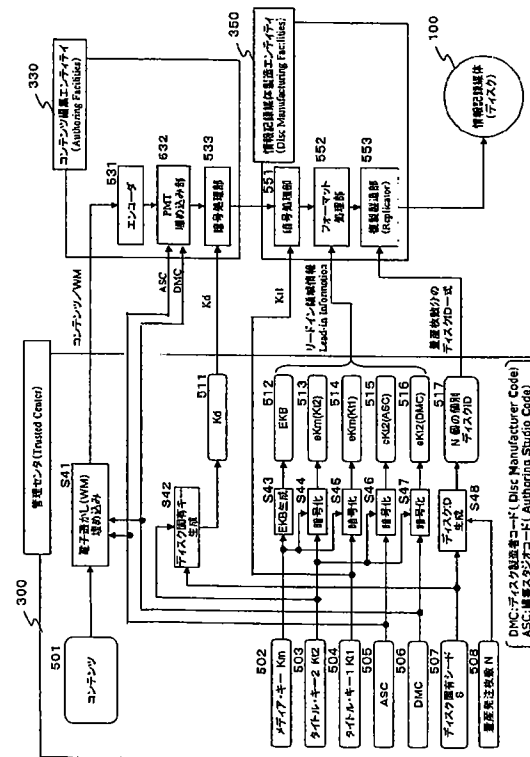
【 図 1 6 】



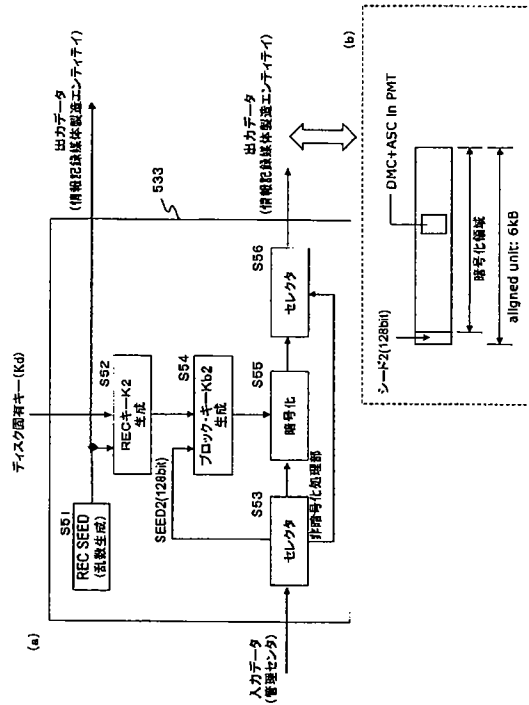
【图 17】



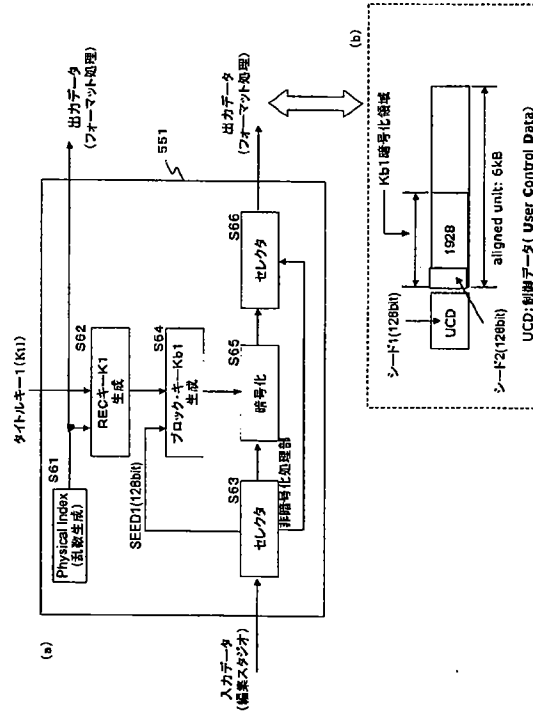
【图 18】



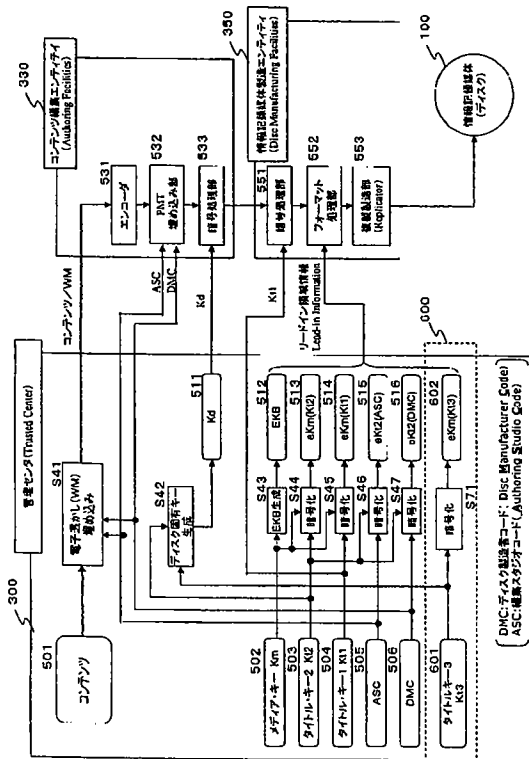
【図 19】



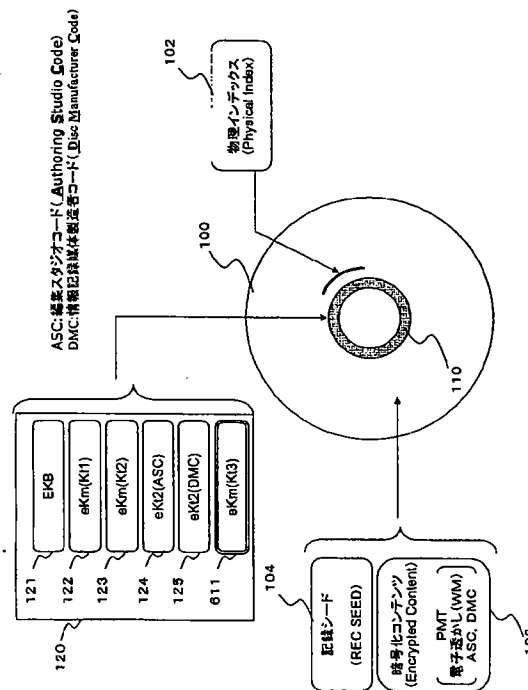
【図 20】



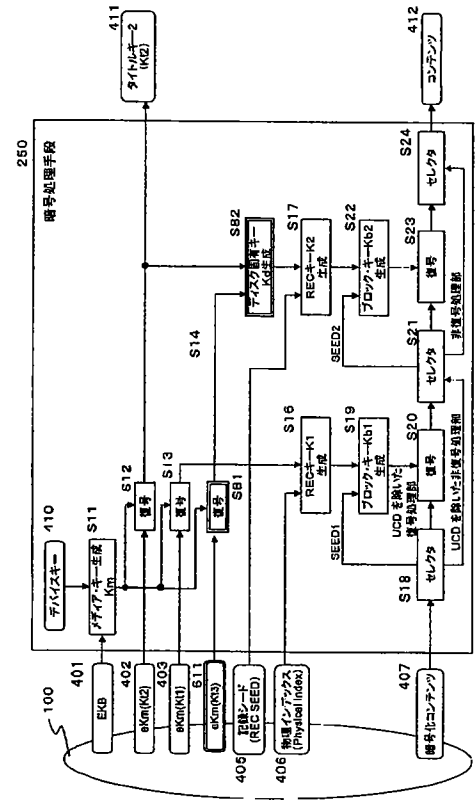
【図 21】



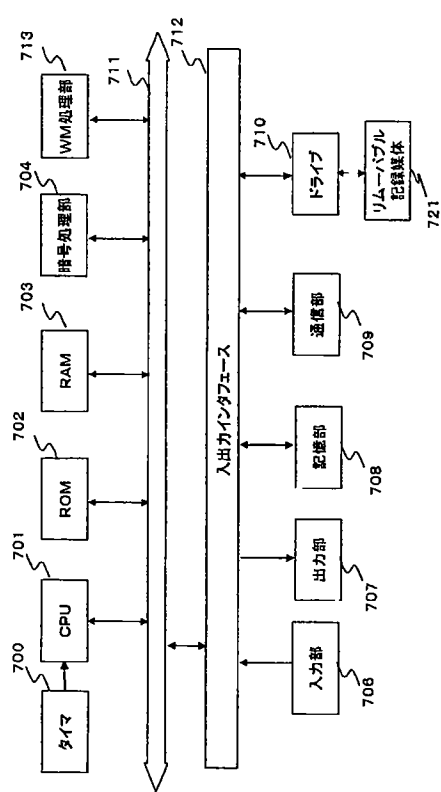
【図 22】



【図 2 3】



【図 2 4】



 フロントページの続き

(51)Int. Cl. ⁷	F I	テーマコード (参考)
	G 1 1 B 27/00	A
	H 0 4 L 9/00	6 0 1 A
	H 0 4 L 9/00	6 0 1 E

(72)発明者 村松 克美
 東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 高島 芳和
 東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 米満 潤
 東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B017 AA06 BA09 BB10 CA16
 5D044 BC03 CC06 DE49 DE50 FG18 GK12 GK17 HL08
 5D110 AA15 AA29 BB06 BB29 CA10 DA08 DB03 DE04
 5J104 AA07 AA12 AA16 EA01 EA04 EA15 EA18 JA03 KA02 KA04
 KA05 KA15 LA06 MA05 NA02 NA27 NA37 PA14